云审计服务

最佳实践

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 CTS 最佳实践汇总

本文汇总了基于云审计服务（CTS，Cloud Trace Service）常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户轻松构建基于CTS的审计事件业务。

表 1-1 CTS 最佳实践一览表

最佳实践	说明
结合函数工作流对登录/登出进行审计分析	本章节介绍如何通过CTS云审计服务，完成对公有云账户的各个云服务资源操作和结果的实时记录。 通过在函数工作流服务中创建CTS触发器获取订阅的资源操作信息，经由自定义函数对资源操作的信息进行分析和处理，产生告警日志。再由SMN消息通知服务通过短信和邮件推送告警信息，通知业务人员进行处理。
CTS安全最佳实践	本章节提供了CTS使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。
通过云日志服务LTS存储和查询审计事件	本章节以“创建云服务器”（操作名称：createServer）为例，为您介绍如何通过云日志服务（LTS）存储和查询审计事件。
使用云审计服务监控“创建IAM用户”操作	本章节为您介绍如何通过云审计服务的操作审计和关键操作通知功能，对“创建IAM用户”操作进行监控，并通过邮件通知方式进行告警。
使用云审计服务监控AccessKey的使用	本章节为您介绍如何通过云审计服务的操作审计功能和转储审计日志到LTS功能，对AccessKey相关事件进行监控，并使用LTS日志告警功能发出告警。
使用云审计服务监控华为云账号的使用	本章节为您介绍如何通过云审计服务的操作审计功能和转储审计日志到LTS功能，对华为云账号进行监控，并使用LTS日志告警功能发出告警。
下载云审计服务记录的操作事件	本章节为您介绍如何在云审计服务（CTS）、对象存储服务（OBS）和云日志服务（LTS）中下载操作审计的事件。

最佳实践	说明
通过云审计服务监控DEW密钥的使用	本章节为您介绍如何通过云审计服务的操作审计功能和筛选查询事件功能，对DEW密钥的使用情况进行监控。
将云审计记录的事件持续投递到指定服务	本章节将为您介绍如何将云审计记录的事件持续投递到对象存储服务（OBS）和云日志服务（LTS）。

2 结合函数工作流对登录/登出进行审计分析

2.1 案例概述

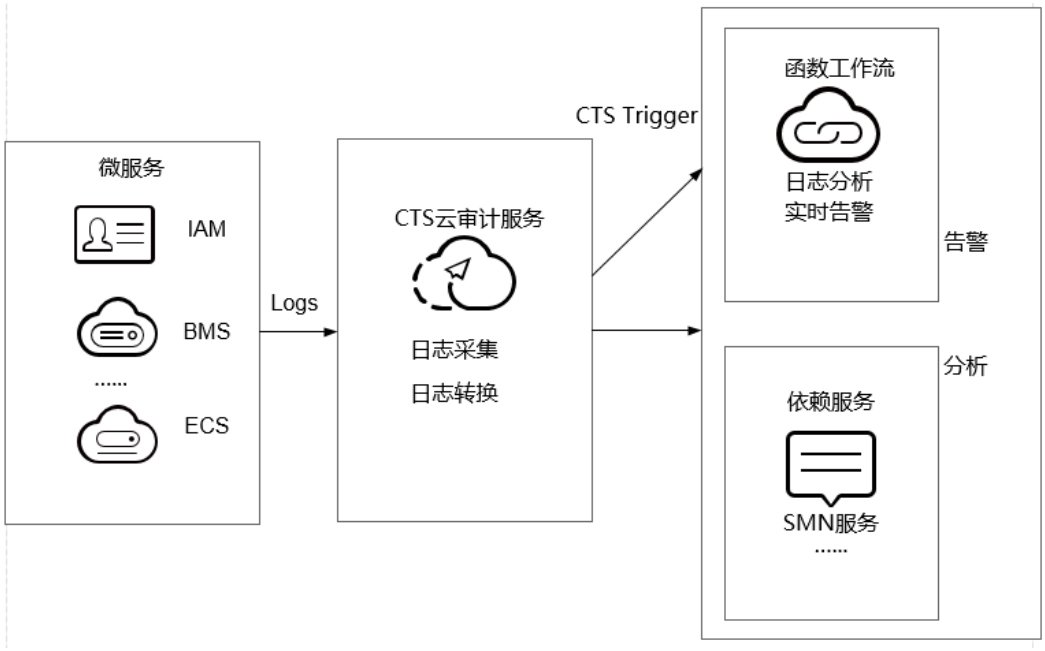
场景介绍

通过CTS云审计服务，完成对公有云账户对各个云服务资源操作动作和结果的实时记录。

通过在函数工作流服务中创建CTS触发器获取订阅的资源操作信息，经由自定义函数对资源操作的信息进行分析和处理，产生告警日志。

SMN消息通知服务通过短信和邮件推送告警信息，通知业务人员进行处理。处理流程如图2-1所示。

图 2-1 处理流程



案例价值点

- 通过CTS云审计服务，快速完成日志分析，对指定IP进行过滤。
- 基于serverless无服务架构的函数计算提供数据加工、分析，事件触发，弹性伸缩，无需运维，按需付费。
- 结合SMN消息通知服务提供日志、告警功能。

2.2 准备

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**。

----结束

创建委托

步骤1 登录**统一身份认证服务控制台**，在左侧导航栏单击“委托”，进入“委托”界面。

步骤2 单击“创建委托”，进入“创建委托”界面。

步骤3 填写委托信息。

- 委托名称：输入您自定义的委托名称，此处以“serverless_trust”为例。
- 委托类型：选择“云服务”。
- 云服务：选择“函数工作流 FunctionGraph”。
- 持续时间：选择“永久”。
- 描述：填写描述信息。

步骤4 单击“下一步”，进入委托选择页面，在“配置权限”界面勾选“CTS Administrator”和“SMN Administrator”。

说明

- SMN Administrator：拥有该权限的用户可以对SMN服务下的资源执行任意操作。
- 选择“CTS Administrator”，由于该策略有依赖，在勾选时，还会自动勾选依赖的策略：Tenant Guest。

步骤5 单击“下一步”，根据实际业务需求选择资源授权范围，单击“确定”，完成权限委托设置。

----结束

告警消息推送

- 在SMN消息通知服务创建主题，此处以主题名称cts_test为例，创建过程请参考**创建主题**。
- 在SMN消息通知服务订阅主题，用于将告警消息推送至该主题下的订阅终端，此处以添加邮件订阅终端为例，订阅cts_test主题，订阅过程请参考**订阅主题**。

  说明

  订阅主题可选择通过邮件、短信、HTTP/HTTPS等形式推送告警消息。

  本案例中推送告警消息的事件是：当日志事件通过CTS触发器触发函数执行时，函数中过滤白名单告警日志，产生的告警消息推送至SMN主题的订阅终端。

2.3 构建程序

本案例提供了实现告警日志功能的程序包，使用空白模板创建函数，用户可以**下载（index.zip）**学习使用。

创建功能函数

创建实现日志提取功能的函数，将**示例代码**包上传。创建过程请参考创建函数，运行时语言选择“Python2.7”，委托名称选择**创建委托**中的“serverless_trust”。

函数实现的功能是：将收到的日志事件数据进行分析，过滤白名单功能，对非法IP登录/登出，进行SMN消息主题邮件告警。形成良好的账户安全监听服务。

设置环境变量

在函数配置页签需配置环境变量，设置SMN主题名称，说明如**表2-1**所示。

表 2-1 环境变量说明表

环境变量	说明
SMN_Topic	SMN主题名称。
RegionName	Region域
IP	白名单

环境变量的设置过程请参考**使用环境变量**。

2.4 添加事件源

选择**准备**中开通的CTS云审计服务，创建CTS触发器，CTS触发器配置如**图2-2**所示。

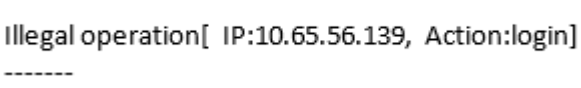
图 2-2 创建 CTS 触发器

CTS云审计服务监听IAM服务中user资源类型，监听login、logout操作。

2.5 处理结果

若用户触发账号的登录/登出操作，订阅服务类型日志被触发，日志会直接调用用户函数，通过函数代码对当前登录/出的账号进行IP过滤，若不在白名单内，可收到SMN发送的通知消息邮件，如图2-3所示。

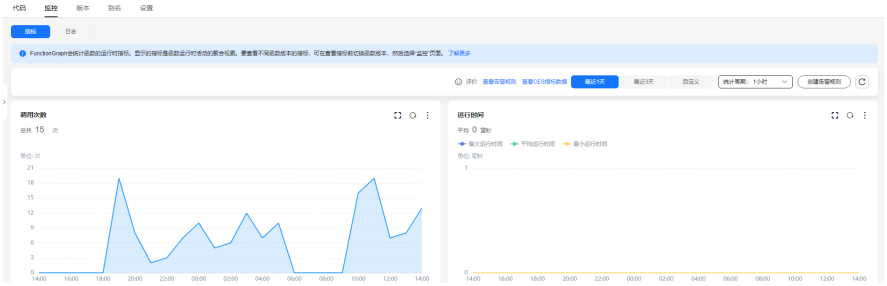
图 2-3 告警消息邮件通知



邮件信息中包含非法请求ip地址和用户执行的动作（ login/logout ）。

可以通过函数指标查看函数的调用情况，如图2-4所示。

图 2-4 函数指标



3 CTS 安全最佳实践

安全性是华为云与您的共同责任。华为云负责云服务自身的安全，提供安全的云；作为租户，您应当使用云服务提供的安全能力对业务及数据安全保护，安全地使用云。详情请参见**责任共担**。

本文提供了CTS使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。根据该指导文档您可以持续评估CTS资源的安全状态，更好的组合使用CTS提供的多种安全能力，保护存储在CTS内的数据不泄露、不被篡改，以及数据传输过程中不泄露、不被篡改。

本文从以下几个维度给出建议，您可以评估CTS使用情况，并根据业务需要在本指导的基础上进行安全配置。

3.1 启用云审计服务，便于云上用户对操作的事后审查

云审计服务（Cloud Trace Service，CTS），是华为云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、资源跟踪和问题定位等常见应用场景。

您开通云审计服务并创建和配置追踪器后，CTS可记录CTS的管理事件审计。详情请参考**开通云审计**。

云审计服务支持多维度资源查询，便于云上用户事后精准审查定位。

图 3-1 事件列表

3.2 开启云审计服务配置 OBS 桶，将审计事件归档 OBS 永久存储

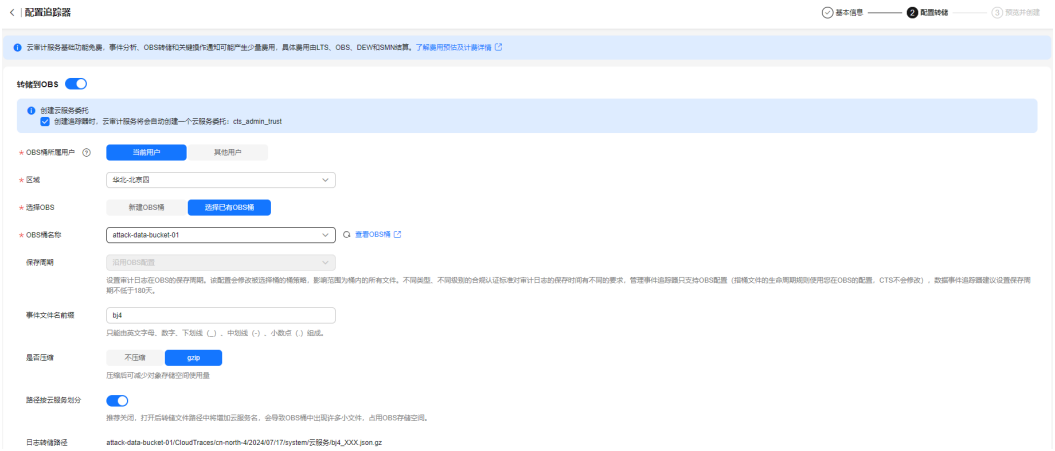
由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶（建议您配置独立OBS桶并配置DEW加密存储专门用于归档

审计事件）。当云上资源发生变化时，CTS服务将审计事件归档至OBS的桶，操作详情参考：**追踪器配置OBS转储**。

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**。

图 3-2 配置转储



3.3 开启云审计服务，请配置审计事件通知

云审计提供了事件通知能力，便于用户实时接收重点审计事件通知，操作详情：**启用审计事件通知**。当您在比较关注对华为云的资源增加删除比较关注时，您可启用云审计事件通知规则并配置相应资源的服务类型、资源类型、动作，云审计服务将实时根据您配置邮件或短信的规则通过消息通知服务（SMN）发送通知。以ECS服务为例，在云审计界面选择事件通知，选择ECS服务，选择ECS的资源类型ecs，选择对应的action，然后订阅SMN通知即可。具体操作和邮件通知范例如下图：

图 3-3 关键操作通知

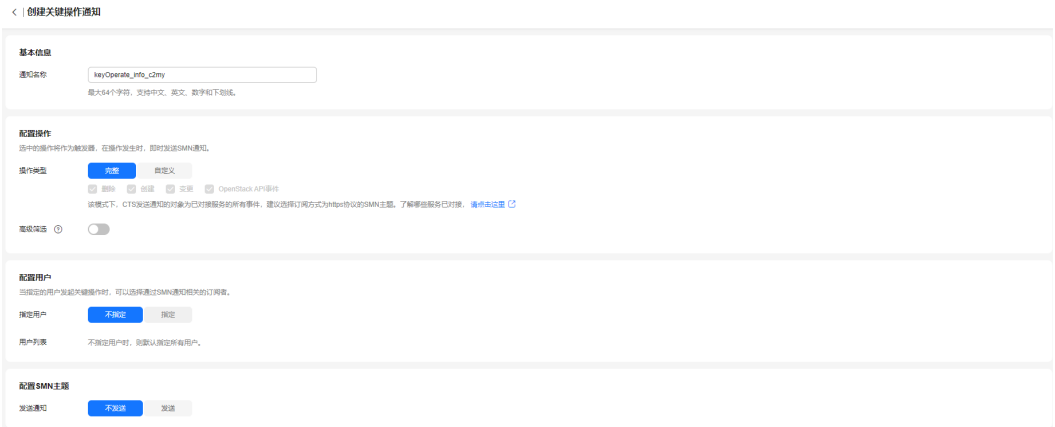


图 3-4 邮件通知

3.4 建议对不同角色的 IAM 用户仅设置最小权限，避免权限过大导致数据泄露

为了更好的进行权限隔离和管理，建议您配置独立的IAM管理员，授予IAM管理员IAM策略的管理权限。

IAM管理员可以根据您业务的实际诉求创建不同的用户组，用户组对应不同的数据访问场景。

通过将用户添加到用户组并将IAM策略绑定到对应用户组，IAM管理员可以为不同职能部门的员工按照最小权限原则授予不同的数据访问权限，详情请参见**CTS权限管理**。

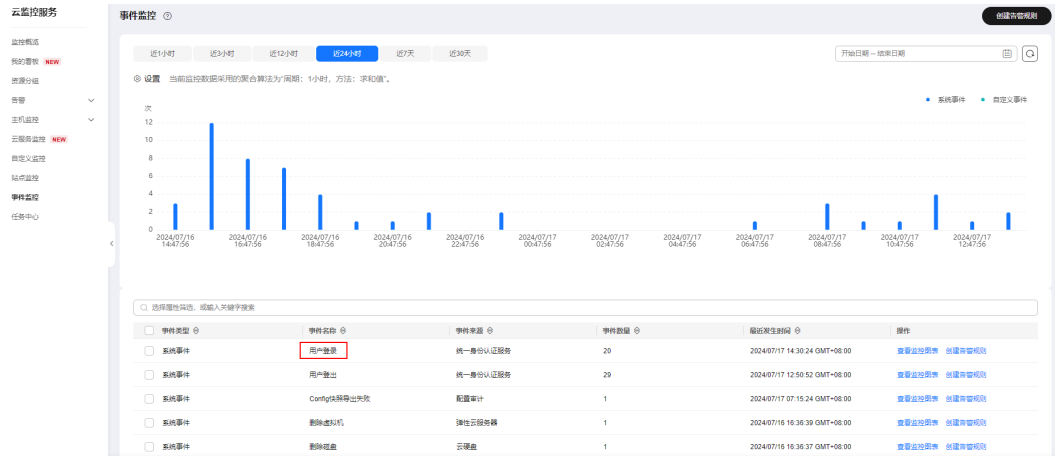
3.5 使用云监控服务对重点审计事件进行实时监控告警

云审计会将华为云ECS、VPC、EVS等云服务重点审计事件如: deleteServer、deleteVpc、deleteVolume等发送CES事件监控中，您可使用该服务监控自己的云上资源操作频率，执行自动实时监控、告警和通知操作，帮助您实时掌握特定云服务云上资源操作频次、操作返回状态、发生时间等信息。云监控服务不需要开通，当启用CTS服务后，CTS服务自动将特定云服务审计事件上报CES。

关于云监控服务的更多介绍，请参见**云监控服务产品介绍**。

下面以IAM服务用户登录、登出事件为例，选择CES的事件监控，选择用户登录时间。

图 3-5 事件监控



设置告警策略，可以设置一个事件周期，阈值超过设置可视为此用户登录异常产生。

图 3-6 告警策略

3.6 使用最新版本的 SDK 获得更好的操作体验和更强的安全能力

建议客户升级SDK并使用最新版本，从客户侧对您的数据和CTS使用过程提供更好的保护。

最新版本SDK在各语言对应界面下载，请参见**CTS SDK**。

您可以在SDK列表中查看CTS支持的SDK，在GitHub仓库查看SDK更新历史、获取安装包以及查看指导文档。

4 通过云日志服务 LTS 存储和查询审计事件

云审计服务（CTS）直接对接华为云上的其他服务，实时记录用户对云服务资源的操作动作和结果，还支持将记录内容以事件文件形式保存至OBS桶或LTS日志流中。本文以“创建云服务器”（操作名称：createServer）为例，为您介绍如何通过云日志服务（LTS）存储和查询审计事件。

前提条件

请确保已开通云审计服务。具体操作，请参见**开通云审计服务**。

配置 LTS 转储

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“追踪器”，进入追踪器信息页面。

步骤3 在管理类追踪器(system)的右侧，单击操作下的“配置”。

图 4-1 追踪器配置

步骤4 设置追踪器的基本信息，单击“下一步”。

参数名称	说明	本实践要求
追踪器名称	默认为system，不可修改。	system

参数名称	说明	本实践要求
企业项目	如果您的账号开通了企业项目管理功能，则需要在此处选择一个企业项目。 **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**。	default
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**。	不勾选

步骤5 在配置转储页面，打开“转储到LTS”开关，系统会自动在LTS创建日志组：CTS，日志流：system-trace，操作事件将转储到日志流中。

图 4-2 开启转储到 LTS 功能

步骤6 单击“下一步 > 配置”，完成配置system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。

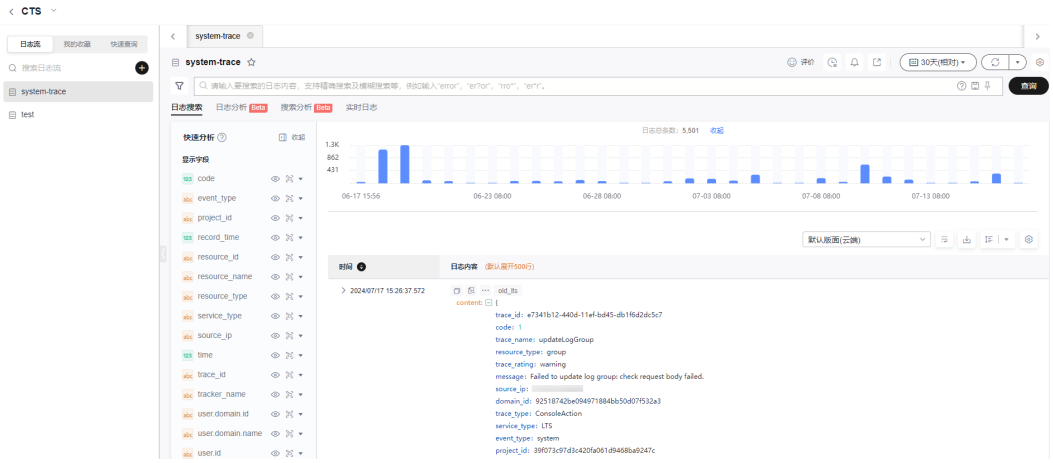
----结束

在云日志服务 LTS 查询审计事件

步骤1 在追踪器页面，单击system追踪器右侧的LTS日志流名称，进入到system-trace日志流详情页面。

图 4-3 单击日志流名称

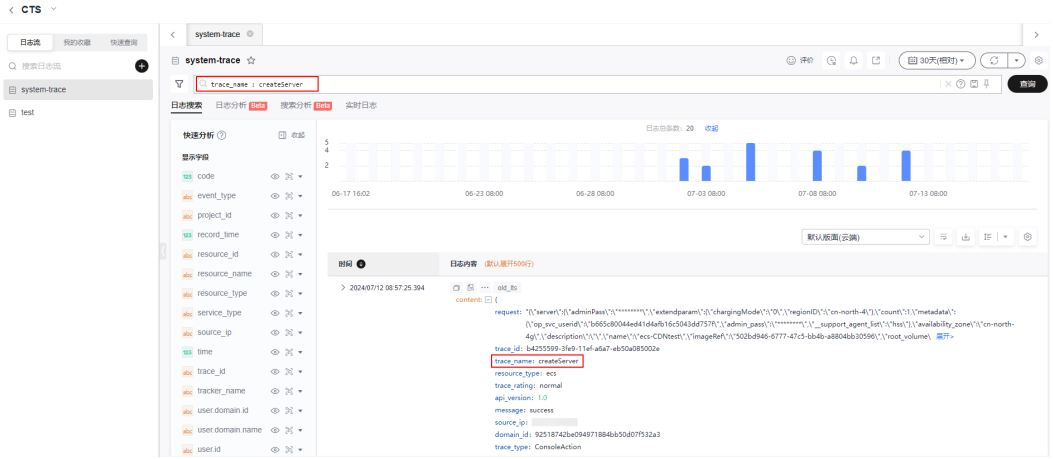
图 4-4 system-trace 日志流页面



步骤2 单击右上角的“15分钟(相对)”，设置查询的时间范围。

步骤3 在搜索框中输入trace_name : createServer，单击查询，查询创建云服务器的事件详情。

图 4-5 搜索 createServer 事件



----结束

5 使用云审计服务监控“创建 IAM 用户”操作

统一身份认证(IAM)是华为云提供权限管理的基础服务，可以帮助您安全地控制华为云服务和资源的访问权限。使用IAM的用户管理功能，给员工或应用程序创建IAM用户，可以将资源分配给不同的员工或者应用程序使用。

云审计服务支持对IAM的关键操作进行收集、存储和查询，用于用户后续进行安全分析、合规审计、资源跟踪和问题定位等。

本章为您介绍如何通过云审计服务的操作审计和关键操作通知功能，对“创建IAM用户”操作进行监控并通过邮件通知方式进行告警。

使用限制

统一身份认证(IAM)属于全局级服务，需要在中心region（北京四）的云审计控制台配置关键操作通知，才能使用云审计服务的关键操作通知功能。

准备工作

1. 为用户添加云审计服务（CTS）操作权限。
   - 如果您是以主账号登录华为云，请跳到下一个任务。
   - 如果您是以IAM用户登录华为云，需要联系CTS管理员（主账号或admin用户组中的用户）对IAM用户授予CTS FullAccess权限。授权方法请参见**给IAM用户授权**。
2. 开通消息通知服务（SMN），并创建主题（本实践要求主题的名称为“cts-test”），添加订阅（本实践要求订阅的协议选择“邮件”），才能在CTS控制台使用关键操作消息通知功能。具体操作，请参见**创建主题**和**添加订阅**。

   说明

   使用消息通知服务（SMN）创建主题、添加邮件订阅，这会产生额外费用，SMN的计费详情请参考**产品价格详情**。

步骤一：开通云审计服务并配置 system 追踪器

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“追踪器”，进入追踪器界面。

步骤3 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。

步骤4 在管理类追踪器(system)的右侧，单击操作下的“配置”。

图 5-1 追踪器配置

步骤5 设置追踪器的基本信息，单击“下一步”。

参数	参数说明	本实践要求
追踪器名称	默认为system，不可修改。	system
企业项目	如果您的账号开通了企业项目管理功能，则需要在此处选择一个企业项目。 **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**。	default
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**。	不勾选

步骤6 在配置转储页面，您可以设置转储功能。本实践无需使用转储功能，所以关闭“转储到OBS”开关、关闭“转储到LTS”开关。

步骤7 单击“下一步 > 配置”，完成配置system追踪器。追踪器配置成功后，您可以在追踪器页面查看配置的追踪器的详细信息。

----结束

步骤二：创建关键操作通知

步骤1 在云审计控制台，单击左侧导航栏的“关键操作通知”。

步骤2 在关键操作通知界面，单击“创建关键操作通知”。

步骤3 参照下表中的本实践要求参数，设置关键操作通知的参数信息，单击“确定”。

图 5-2 创建关键操作通知

表 5-1 设置参数信息

参数	参数说明	本实践要求
通知名称	填写通知的名称，用于标识和区分关键操作通知。	对创建IAM用户操作告警
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。	自定义
操作列表	当操作类型选择“自定义”时，可以自定义选择触发通知的操作范围。	服务类型选择：IAM 资源类型选择：user 操作名称选择：createUser
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。	不设置
指定用户	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。	不指定
发送通知	当选择“发送”通知时，需要设置创建云服务委托和SMN主题。当选择“不发送”通知时，则无需配置。	发送
创建云服务委托	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）。	勾选
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。	cts-test

----结束

步骤三：执行“创建 IAM 用户”操作后，验证触发告警

步骤1 登录**IAM控制台**，创建一个IAM用户。具体操作，请参见**创建IAM用户**。

步骤2 等待邮件终端接收“对创建IAM用户操作告警”邮件通知。

步骤3 成功接受到“对创建IAM用户操作告警”邮件，实现通过云审计服务监控“创建IAM用户”操作。

尊敬的华为云用户 [redacted]：

您的资源 **test** 在 IAM 服务于 2024-10-29 17:32:44 GMT+0800 发生操作，请您关注！详见云审计服务

区域：华北-北京四

操作事件：createUser

操作对象：IAM(test, 4fcb[redacted]09da)// 服务名称(资源名称， 资源 ID)

操作时间：2024-10-29 17:32:44 GMT+0800

操作用户：[redacted]

操作记录内容：

{
"code":201,
"domain_id":"7e0d[redacted]7cba",
"operation_id":"KeystoneCreateUser",
"project_id":"0706[redacted]286e",
"read_only":false,
"record_time":"2024-10-29 17:32:44 GMT+0800",
"request":"{"user":{"domain_id":"7e0d[redacted]7cba","pwd_status":false,"xuser_id":"","name":"test","mobile":"","xuserId":"","description":"","groups":[],"xuser_type":"","access_mode":"programmatic","em
"resource_account_id":"7e0d[redacted]7cba",
"resource_id":"4fcb[redacted]09da",
"resource_name":"test",
"resource_type":"user",
"service_type":"IAM",
"source_ip":"124.71.93.164",
"time":"2024-10-29 17:32:44 GMT+0800",
"trace_id":"c0453409-95d8-11ef-827a-4ba7d5c48b93",
"trace_name":"createUser",
"trace_rating":"normal",
"trace_type":"ConsoleAction",
"user":"{"access_key_id":"HS[redacted]4Y","account_id":"7e0d[redacted]7cba","domain":{"id":"7e0d[redacted]7cba","name":"[redacted]"},"id":"f369[redacted]1214","name"
"user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36"
}

感谢您对华为云的支持！

----结束

常见问题相关链接

使用IAM用户无法开通CTS怎么办?

向主题推送消息后，订阅者为什么没有收到消息?

6 使用云审计服务监控 AccessKey 的使用

访问密钥（AccessKey）包括访问密钥ID（AccessKey ID）和访问密钥密码（AccessKey Secret），用于标识用户和验证用户的密钥。AccessKey泄露会威胁您资源的安全。

云审计服务帮助您监控AccessKey相关事件，以便您发现AccessKey使用异常时快速应对。

本章为您介绍如何通过云审计服务的操作审计功能和转储审计日志到LTS功能，对AccessKey相关事件进行监控，并使用LTS日志告警功能发出告警。

准备工作

为用户添加云审计服务（CTS）和云日志服务（LTS）操作权限。

- 如果您是以主账号登录华为云，请跳到**步骤一：开通云审计服务并配置system追踪器**。
- 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**。
- 联系LTS管理员（主账号或admin用户组中的用户）对IAM用户授予LTS FullAccess权限。

  说明

  使用云日志服务（LTS）日志存储功能，这会产生额外费用，LTS的计费详情请参考**产品价格详情**。

步骤一：开通云审计服务并配置 system 追踪器

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“追踪器”，进入追踪器界面。

步骤3 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。

步骤4 在管理类追踪器(system)的右侧，单击操作下的“配置”。

图 6-1 追踪器配置

步骤5 设置追踪器的基本信息，单击“下一步”。

参数	参数说明	本实践要求
追踪器名称	默认为system，不可修改。	system
企业项目	如果您的账号开通了企业项目管理功能，则需要在此处选择一个企业项目。 **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**。	default
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**。	不勾选

步骤6 在配置转储页面，打开“转储到LTS”开关，系统会自动在LTS创建日志组：CTS，日志流：system-trace，操作事件将转储到日志流中。

图 6-2 开启转储到 LTS 功能

步骤7 单击“下一步 > 配置”，完成配置system追踪器。追踪器配置成功后，您可以在追踪器页面查看配置的追踪器的详细信息。

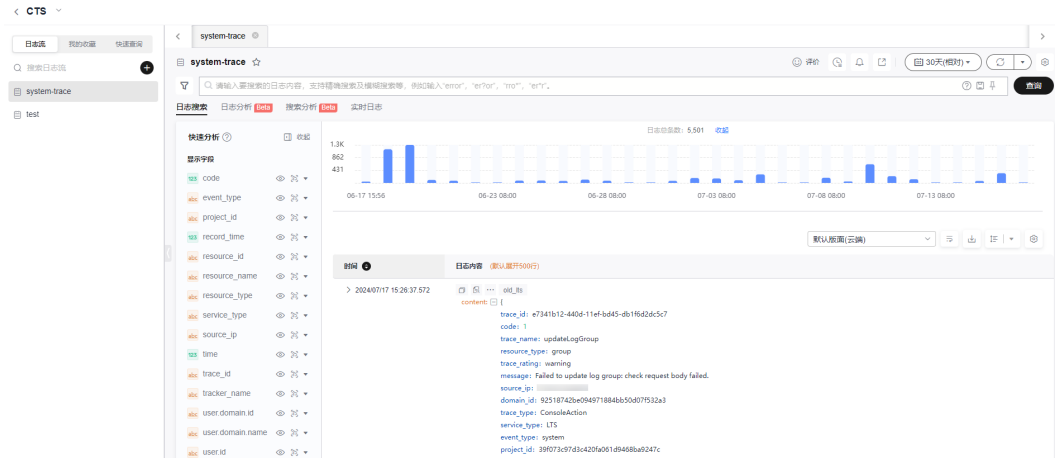
----结束

步骤二：在 LTS 中查询事件

步骤1 在云审计控制台的追踪器页面，单击system追踪器右侧的LTS日志流名称，进入到system-trace日志流详情页面。

图 6-3 单击日志流名称

图 6-4 system-trace 日志流页面



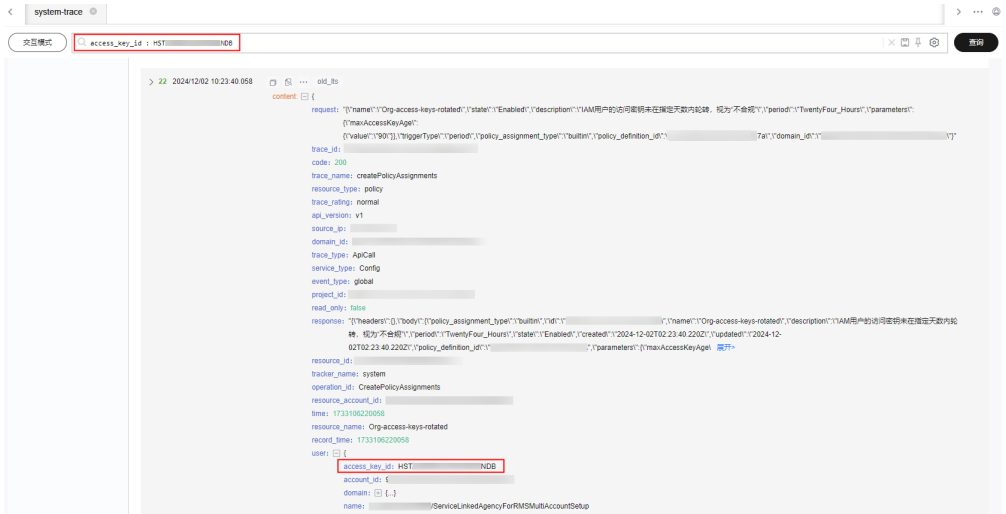
步骤2 单击右上角的“15分钟(相对)”，设置查询的时间范围。

步骤3 在搜索框中输入access_key_id:*{access_key_id}*，单击“查询”。

说明

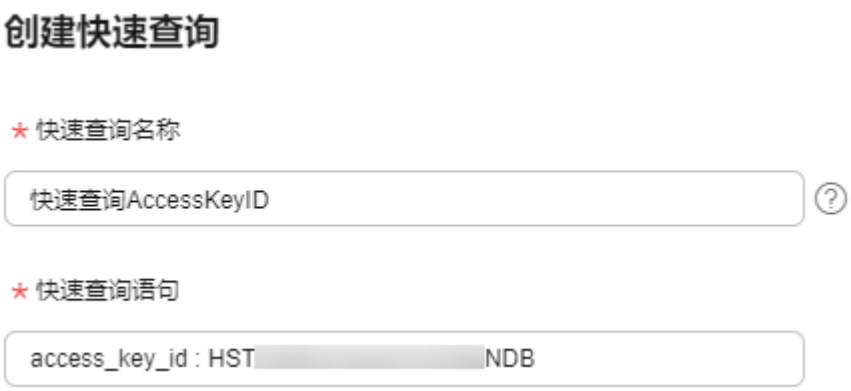
- *{access_key_id}*请替换为您自己的AccessKey ID。
- 查询日志时报错提示：access_key_id 字段未配置字段索引，不支持查询该字段。
  - 可能原因：用户没有配置字段索引。
  - 解决方法：请您在索引配置中创建access_key_id字段的字段索引，重新执行查询语句。配置说明请参考**配置索引**。

图 6-5 搜索 access_key_id



步骤4 单击搜索框右侧的图标，可以创建快速查询。输入快速查询名称后，单击“确定”。

图 6-6 创建快速查询



步骤5 创建快速查询后，您可以在云日志服务控制台的CTS日志组页面直接选择该快速查询。

图 6-7 快速查询

----结束

步骤三：在 LTS 中配置告警

步骤1 在云日志服务控制台的CTS日志组页面，单击右上方的图标，可以添加告警。

步骤2 在新建告警规则面板配置相关参数，然后单击“确定”。配置说明请参考**配置日志告警规则**。

步骤3 设置告警规则后，满足触发条件即可收到告警通知，例如您可以设置：如果access_key_id在5分钟内被使用过，则上报告警。

步骤4 添加的告警可以在云日志服务控制台“日志告警”页面进行管理。

----结束

7 使用云审计服务监控华为云账号的使用

华为云账号是您的华为云资源归属、资源使用计费的主体。华为云账号泄露会威胁您所有资源的安全。您可以使用云审计服务监控华为云账号的使用，设置告警保障您的华为云账号下资源的安全。

本章为您介绍如何通过云审计服务的操作审计功能和转储审计日志到LTS功能，对华为云账号进行监控，并使用LTS日志告警功能发出告警。

准备工作

为用户添加云审计服务（CTS）和云日志服务（LTS）操作权限。

- 如果您是以主账号登录华为云，请跳到**步骤一：开通云审计服务并配置system追踪器**。
- 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**。
- 联系LTS管理员（主账号或admin用户组中的用户）对IAM用户授予LTS FullAccess权限。

说明

使用云日志服务（LTS）日志存储功能，这会产生额外费用，LTS的计费详情请参考**产品价格详情**。

步骤一：开通云审计服务并配置 system 追踪器

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“追踪器”，进入追踪器界面。

步骤3 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。

步骤4 在管理类追踪器(system)的右侧，单击操作下的“配置”。

图 7-1 追踪器配置

步骤5 设置追踪器的基本信息，单击“下一步”。

参数	参数说明	本实践要求
追踪器名称	默认为system，不可修改。	system
企业项目	如果您的账号开通了企业项目管理功能，则需要在此处选择一个企业项目。 **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**。	default
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**。	不勾选

步骤6 在配置转储页面，打开“转储到LTS”开关，系统会自动在LTS创建日志组：CTS，日志流：system-trace，操作事件将转储到日志流中。

图 7-2 开启转储到 LTS 功能

步骤7 单击“下一步 > 配置”，完成配置system追踪器。追踪器配置成功后，您可以在追踪器页面查看配置的追踪器的详细信息。

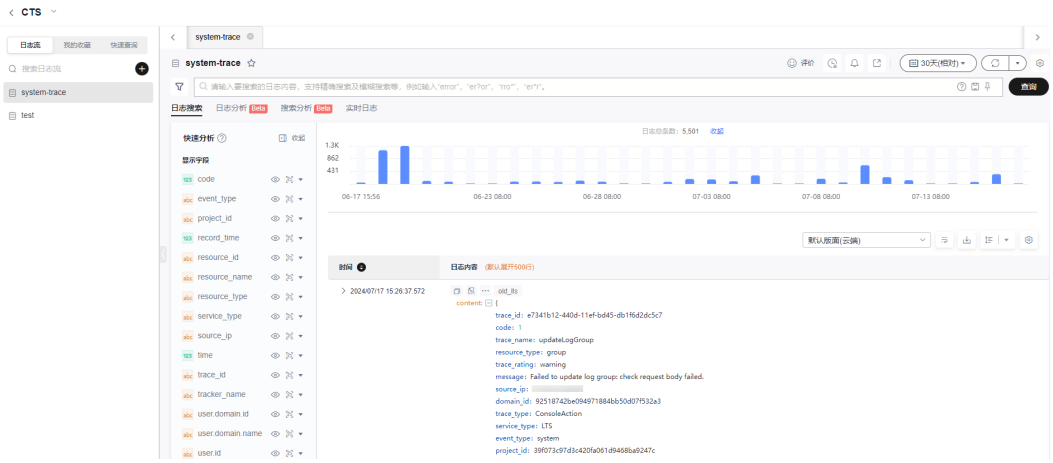
----结束

步骤二：在 LTS 中查询事件

步骤1 在云审计控制台的追踪器页面，单击system追踪器右侧的LTS日志流名称，进入到system-trace日志流详情页面。

图 7-3 单击日志流名称

图 7-4 system-trace 日志流页面



步骤2 单击右上角的“15分钟(相对)”，设置查询的时间范围。

步骤3 在搜索框中输入user.name:*{username}*，单击“查询”。

说明

- 执行搜索与分析前，需要将上报的日志进行结构化配置和索引配置，详细请参考**设置云端结构化解析日志**和**设置LTS日志索引配置**。
- *{username}*请替换为您自己的用户名称。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”。

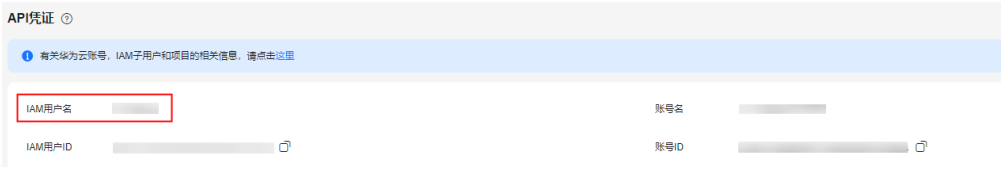
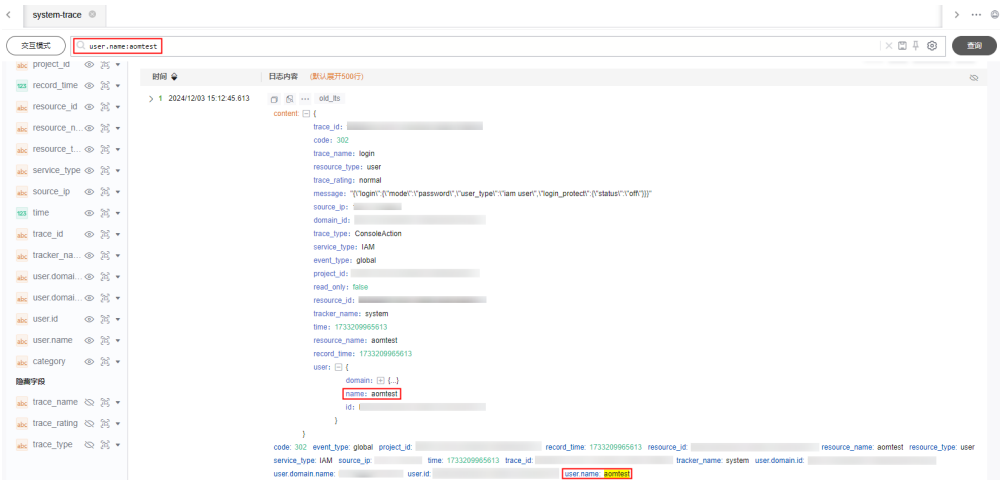


图 7-5 搜索 user.name



步骤4 单击搜索框右侧的图标，可以创建快速查询。输入快速查询名称后，单击“确定”。

图 7-6 创建快速查询

步骤5 创建快速查询后，您可以在云日志服务控制台的CTS日志组页面直接选择该快速查询。

----结束

步骤三：在 LTS 中配置告警

步骤1 在云日志服务控制台的CTS日志组页面，单击右上方的图标，可以添加告警。

步骤2 在新建告警规则面板配置相关参数，然后单击“确定”。配置说明请参考**配置日志告警规则**。

步骤3 设置告警规则后，满足触发条件即可收到告警通知。

步骤4 添加的告警可以在云日志服务控制台“日志告警”页面进行管理。

----结束

8 下载云审计服务记录的操作事件

云审计服务默认为每个华为云账号记录最近7天的操作事件，最近7天的操作事件仅支持通过云审计控制台查询，您可以在云审计控制台导出本次查询结果的所有事件。在您没有配置转储前，云审计控制台对用户的操作事件日志保留7天，过期自动删除，在配置转储后也无法查看。

如果您因为审计要求需要获取7天以上的操作事件，或者需要将事件下载到本地进行分析，则必须配置system追踪器转储事件至OBS或LTS，再通过OBS或LTS的数据下载能力将事件以文件形式下载到本地。

本章为您介绍如何在云审计服务（CTS）、对象存储服务（OBS）和云日志服务（LTS）中下载操作审计的事件。

说明

1. 使用对象存储服务（OBS）文件存储功能，这会产生额外费用，以及在OBS桶中下载文件将产生请求费用和流量费用。OBS的计费详情请参考**产品价格详情**。
2. 使用云日志服务（LTS）日志存储功能，这会产生额外费用，LTS的计费详情请参考**产品价格详情**。

在云审计服务 CTS 下载操作事件

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表页面。

步骤3 单击页面上方的“最近1小时”，设置查询的时间范围。

步骤4 单击“导出”按钮，选择“导出全部数据到XLSX”。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。

----结束

在对象存储服务 OBS 下载操作事件

步骤1 在云审计控制台，进入追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的OBS桶（在本案例中，OBS桶的名称为“system-bucket-01”）。

步骤2 单击OBS桶名称“system-bucket-01”，页面跳转到对象存储服务控制台上“system-bucket-01”桶的管理界面。

图 8-1 单击 OBS 桶名称

步骤3 在“system-bucket-01”桶的管理界面左侧的导航栏，单击“对象”。

步骤4 在对象页面，按照事件文件存储路径依次点开文件夹。

事件文件存储路径格式：***OBS桶名>CloudTraces>地区标示>时间标示：年>时间标示：月>时间标示：日>追踪器名称 >服务类型目录***

说明

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”。

步骤5 您可以下载单个对象或批量下载对象。详细操作说明请参考**下载对象**。

- **下载单个对象：**

  在您需要下载的对象右侧单击“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，请单击对象右侧的“更多 > 下载为”。

- **批量下载对象：**

  勾选您需要下载的多个对象，单击对象列表上方的“更多>下载”。

步骤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，通过记事本等txt文档编辑软件即可查看历史操作事件日志信息。

----结束

在云日志服务 LTS 下载操作事件

步骤1 在云审计控制台，进入追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的LTS日志流“CTS/system-trace”。

步骤2 单击日志流名称“CTS/system-trace”，页面跳转到云日志服务控制台上“CTS/system-trace”日志流界面。

图 8-2 单击日志流名称

步骤3 下载日志：单击页面右上方的图标，在弹出的下载日志页面中选择下载方式，下载日志文件到本地。详细操作说明请参考**日志搜索的常用操作**。

----结束

9 通过云审计服务监控 DEW 密钥的使用

华为云数据加密服务（DEW）提供DEW密钥功能，可以帮助用户创建、加密和解密数据加密密钥，以保护云服务中的敏感数据安全。通过云审计服务监控DEW密钥的使用，您可以及时发现异常活动、未授权操作或潜在的安全风险。有效的监控和审计可以帮助您更好地管理和保护DEW密钥，确保数据的安全性和合规性。

本文为您介绍如何通过云审计服务的操作审计功能和筛选查询事件功能，对DEW密钥的使用情况进行监控。

准备工作

为用户添加云审计服务（CTS）操作权限。

- 如果您是以主账号登录华为云，请进行下一个操作：**开通云审计服务并配置system追踪器**。
- 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**。

开通云审计服务并配置 system 追踪器

步骤1 登录**云审计控制台**。

步骤2 单击左侧导航栏的“追踪器”，进入追踪器界面。

步骤3 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。

步骤4 在管理类追踪器(system)的右侧，单击操作下的“配置”。

图 9-1 追踪器配置

步骤5 设置追踪器的基本信息，单击“下一步”。

参数	参数说明	本实践要求
追踪器名称	默认为system，不可修改。	system
企业项目	如果您的账号开通了企业项目管理功能，则需要在此处选择一个企业项目。 **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**。	default
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**。	不勾选

步骤6 在配置转储页面，您可以设置转储功能。本实践无需使用转储功能，所以关闭“转储到OBS”开关、关闭“转储到LTS”开关。

步骤7 单击“下一步 > 配置”，完成配置system追踪器。追踪器配置成功后，您可以在追踪器页面查看配置的追踪器的详细信息。

----结束

场景一：查询创建、删除、启用、禁用 DEW 密钥的记录

步骤1 在云审计控制台，单击左侧导航栏的“事件列表”。

步骤2 单击页面上方的“最近1小时”，设置查询的时间范围。

步骤3 在搜索框中依次查询创建、删除、启用、禁用DEW密钥操作：

- **创建DEW密钥操作：**“云服务：DEW”>“资源类型：cmk”>“事件名称：createKey”。

- **删除DEW密钥操作：**“云服务：DEW”>“资源类型：cmk”>“事件名称：scheduleKeyDeletion”。

- **启用DEW密钥操作：**“云服务：DEW”>“资源类型：cmk”>“事件名称：enableKey”。

- **禁用DEW密钥操作：**“云服务：DEW”>“资源类型：cmk”>“事件名称：disableKey”。

步骤4 在事件列表查看事件的查询结果。

----结束

场景二：查询指定 DEW 密钥的使用情况

步骤1 在云审计控制台，单击左侧导航栏的“事件列表”。

步骤2 单击页面上方的“最近1小时”，设置查询的时间范围。

步骤3 在搜索框中输入需要查询的指定DEW密钥的密钥ID：“资源ID：*{resource_id}*”。

说明

*{resource_id}*请替换为您需要查询的DEW密钥的密钥ID。在云审计服务中，资源ID（Resource ID）就是DEW密钥的密钥ID。

步骤4 在事件列表查看事件的查询结果。

----结束

10 将云审计记录的事件持续投递到指定服务

云审计服务记录了用户对云服务资源新建、修改、删除等操作的详细信息，记录的事件信息会在云审计中保存7天。在您没有配置转储前，云审计控制台对用户的操作事件日志保留7天，过期自动删除，在配置转储后也无法查看。

如果您因为审计要求需要获取7天以上的操作事件，则需要在云审计控制台配置事件转储至OBS或LTS，云审计服务会定期将操作记录同步保存到OBS桶或LTS日志流中进行长期保存。

本章将为您介绍如何将云审计记录的事件持续投递到对象存储服务（OBS）和云日志服务（LTS）。

说明

1. 使用对象存储服务（OBS）文件存储功能，这会产生额外费用，OBS的计费详情请参考**产品价格详情**。
2. 使用云日志服务（LTS）日志存储功能，这会产生额外费用，LTS的计费详情请参考**产品价格详情**。

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，才能使用审计事件上报至CTS功能和审计事件转储至OBS/LTS功能。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。

场景一：将云审计记录的事件转储到 OBS

步骤1 进入**云审计服务页面**。

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

在本案例中，选择“华北-北京四”区域。

步骤3 在左侧导航栏，单击“追踪器”，进入追踪器页面。

步骤4 在system追踪器右侧的操作栏，单击“配置”。

图 10-1 配置 system 追踪器

步骤5 在基本信息页面，设置基本信息，设置完成后，单击“下一步 ”。

表 10-1 设置基本信息

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

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

表 10-2 配置转储至 OBS 参数

参数	参数说明	本案例示例
转储到OBS	云审计服务记录了租户对云服务资源新建、修改、删除等操作的详细信息，记录的事件信息会在云审计中保存7天。如果需要将操作记录保存7天以上，则需要配置事件转储至OBS功能，云审计服务会定期将操作记录同步保存到用户定义的OBS桶中进行长期保存。 开启“转储到OBS”功能后，您就能将审计日志周期性的转储至对象存储服务下的OBS桶。	开启开关
创建云服务委托	用户开启“转储到OBS”功能后，必须勾选“创建云服务委托”，云审计服务将会自动创建一个云服务委托cts_admin_trust，委托授权您使用对象存储服务（OBS）。	勾选“创建云服务委托”
OBS桶所属用户	您可以将事件转储至当前用户或其他用户的OBS桶中，方便统一管理。 ● 选择当前用户：无需授予转储权限。 ● 选择其他用户：转储前需要OBS桶所属用户已经对您当前用户授予转储权限，否则会造成转储失败。授予转储权限的方法请参考**跨租户转储授权**。	选择“当前用户”
选择OBS	您可以选择新建OBS桶或选择已有OBS桶。 ● 新建OBS桶：在您填写一个桶名后系统将自动为您创建一个OBS桶。 **说明** 当前创建的OBS桶是一个单AZ标准存储的私有桶。如果需要其他额外配置，建议提前在OBS服务创建OBS桶，然后“选择已有OBS桶”。 ● 选择已有OBS桶：选择当前区域已创建的OBS桶。	选择“新建OBS桶”
OBS桶名称	OBS桶名称不能为空，仅支持小写字母、数字、“-”和“.”，且长度范围为3-63个字符。禁止两个“.”相邻（如“my..bucket”），禁止“.”和“-”相邻（如“my-.bucket”和“my.-bucket”），禁止使用ip为桶名称。	system-bucket-01
保存周期	不同类型、不同级别的合规认证标准对审计日志的保存时间有不同的要求，当您配置管理类事件追踪器时，保存周期默认“沿用OBS配置”，不支持修改。	沿用OBS配置

参数	参数说明	本案例示例
事件文件名前缀	事件文件名前缀用于标识被转储的事件文件，该字段支持用户自定义，会自动添加在转储事件文件的文件名前端，方便用户快速进行筛选。事件文件名前缀只能由英文字母、数字、下划线(_)、中划线(-)和小数点(.)组成，且长度范围为0-64个字符。 事件文件命名格式： ***操作事件文件前缀_CloudTrace_区域标示/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	FilePrefix
文件校验	开启“文件校验”开关，即可启用事件文件完整性校验功能，云审计服务会在每个小时将上一个小时内所有事件文件的哈希值生成一个摘要文件，并将该摘要文件同步存储至当前追踪器配置的OBS桶中，您可以使用这些文件实现自己的校验解决方案。 事件文件完整性校验详细操作请参考**事件文件完整性校验**。 有关摘要文件的更多信息，请参阅**摘要文件**。	不开启开关
加密事件文件	云审计支持对事件文件加密存储，在转储过程中需使用数据加密服务（简称DEW）中的密钥对存储在OBS桶中的事件文件进行加密。 当OBS所属用户选择“当前用户”时，开启“加密事件文件”开关，云审计会从DEW获取当前用户的密钥ID，在下拉选项可以直接选择密钥。	不开启开关

步骤7 在追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的OBS桶“system-bucket-01”，云审计记录的事件将持续转储到该OBS桶。在OBS桶中查看事件记录的详细操作请参考**在OBS桶中查看历史事件记录**。

图 10-2 OBS 桶名称

----结束

场景二：将云审计记录的事件转储到 LTS

步骤1 进入**云审计服务页面**。

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

在本案例中，选择“华北-北京四”区域。

步骤3 在左侧导航栏，单击“追踪器”，进入追踪器页面。

步骤4 在system追踪器右侧的操作栏，单击“配置”。

图 10-3 配置 system 追踪器

步骤5 在基本信息页面，设置基本信息，设置完成后，单击“下一步”。

表 10-3 设置基本信息

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

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

表 10-4 配置转储至 LTS 参数

参数	参数说明	本案例示例
转储到LTS	云审计服务记录了租户对云服务资源新建、修改、删除等操作的详细信息，控制台事件列表中会保存最近7天的操作记录。如果需要将操作记录保存7天以上，则需要配置事件转储至LTS功能，云审计服务会定期将操作记录同步保存到用户定义的LTS日志流中进行长期保存。 开启“转储到LTS”功能后，您就能将审计日志周期性的转储至云日志服务下的LTS日志流。	开启开关
日志组名称	日志组名称默认为“CTS”，不支持修改。操作事件将转储到“CTS/system-trace”日志流中。	CTS

步骤7 在追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的LTS日志流“CTS/system-trace”，云审计记录的事件将持续转储到该LTS日志流。在LTS日志流中查看事件记录的详细操作请参考**在LTS日志流中查看历史事件记录**。

图 10-4 日志流名称

----结束