

云审计服务

最佳实践

文档版本 01
发布日期 2023-11-10



版权所有 © 华为云计算技术有限公司 2023。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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 结合函数工作流对登录/登出进行审计分析.....	1
1.1 案例概述.....	1
1.2 准备.....	2
1.3 构建程序.....	3
1.4 添加事件源.....	4
1.5 处理结果.....	5

1 结合函数 workflow 对登录/登出进行审计分析

1.1 案例概述

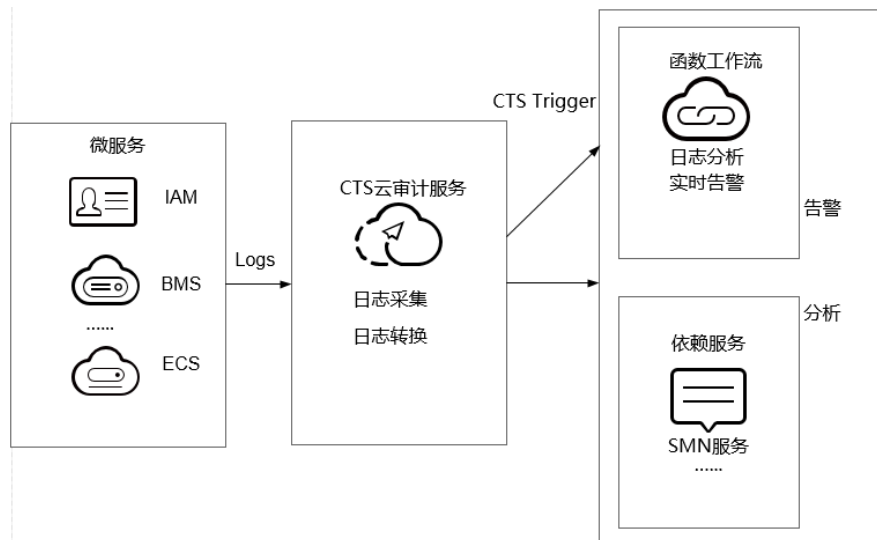
场景介绍

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和结果的实时记录。

通过在函数 workflow 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1-1所示。

图 1-1 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。

1.2 准备

开通 CTS 云审计服务

在云审计服务中开通配置追踪器，配置追踪器完成后，系统立即以新的规则开始记录操作。

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. 在数据事件追踪器信息右侧，单击操作下的“配置”。
 - 追踪操作：配置需要记录日志的数据操作。
 - OBS转储：
 - 当选择是否转储OBS为“转储”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，并配置操作事件文件前缀。
 - 如果配置OBS桶转储为“不转储”时，则无需配置相应参数。
 - 创建新的OBS桶：若打开此开关，在您填写一个桶名后系统将自动为您创建一个OBS桶。若关闭开关，则需要您选择一个已有的OBS桶。
 - 转储OBS桶：您可以直接新建OBS桶或选择已存在的OBS桶。
 - 保存周期：选择转储至OBS桶中日志的保存时长。
 - 事件文件前缀：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。
 - 开启文件校验：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](#)
6. 单击“确定”，完成配置追踪器。

说明

有关配置追踪器的详细信息请参见[追踪器配置](#)。

创建委托

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。
2. 单击“创建委托”，进入“创建委托”界面。
3. 填写委托信息。
 - 委托名称：输入“serverless_trust”。
 - 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”。

- 权限选择：单击“配置权限”，在“配置权限”界面勾选“Tenant Administrator”，单击“确定”。

📖 说明

Tenant Administrator：拥有该权限的用户可以对企业拥有的所有云资源执行任意操作。

4. 单击“确定”，完成权限委托设置。

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。

1.3 构建程序

本案例提供了实现告警日志功能的程序包，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，如[图1-2](#)所示。创建过程请参考[创建函数](#)。

图 1-2 创建函数



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1-1](#)所示。

表 1-1 环境变量说明

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](#)，如图1-3所示。

图 1-3 设置环境变量

环境变量 ⓘ 注意：环境变量会明文展示所输入信息，请防止信息泄露。

键	值	操作
SMN_Topic	cts	删除
RegionName	cn-north-1	删除
IP	192.168.1.2, 10.45.65.48	删除

⊕ 添加环境变量

1.4 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1-4所示。具体操作请参见[使用CTS触发器](#)。

图 1-4 创建 CTS 触发器

创建触发器

触发类型：云审计服务 (CTS)
一个project下CTS触发器可创建数最多10个，现已创建9个。

您已开通CTS服务，可以创建CTS触发器。

* 通知名称：cts_test
支持汉字、字母、数字和下划线，且长度不能超过64个字符

* 自定义操作：您可以添加10个服务，100个操作。了解操作详情，[请点击这里](#)

服务类型	资源类型	操作名称	操作
IAM	user	login logout	删除

⊕ 添加自定义操作

确定 取消

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

1.5 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1-5所示。

图 1-5 告警消息邮件通知

```
Illegal operation[ IP:10.65.56.139, Action:login]
```

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1-6所示。

图 1-6 函数指标

