云审计服务

最佳实践

文档版本 01

发布日期 2024-05-21

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 结合函数工作流对登录/登出进行审计分析

1.1 案例概述

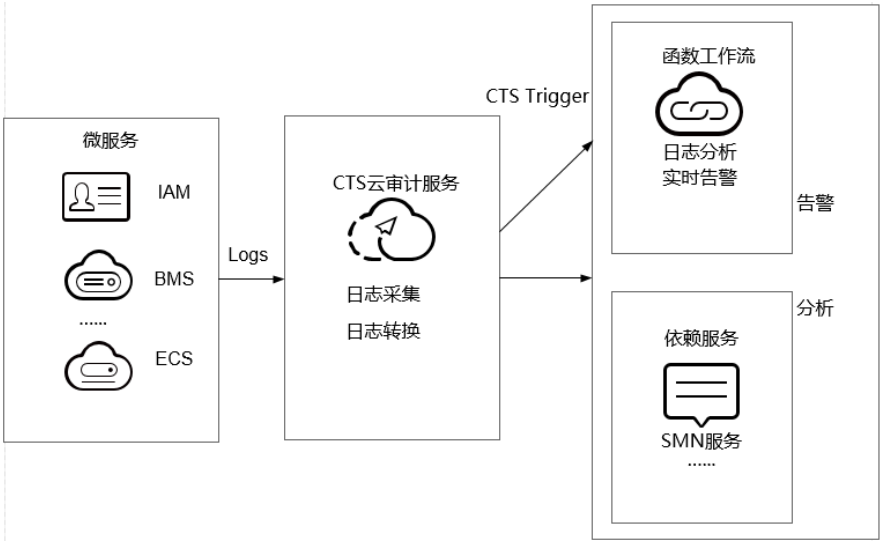
场景介绍

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

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

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

2 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。

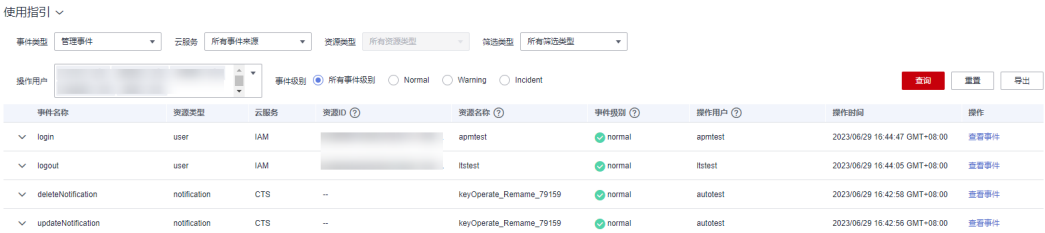
2.1 启用云审计服务，便于云上用户对操作的事后审查

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。

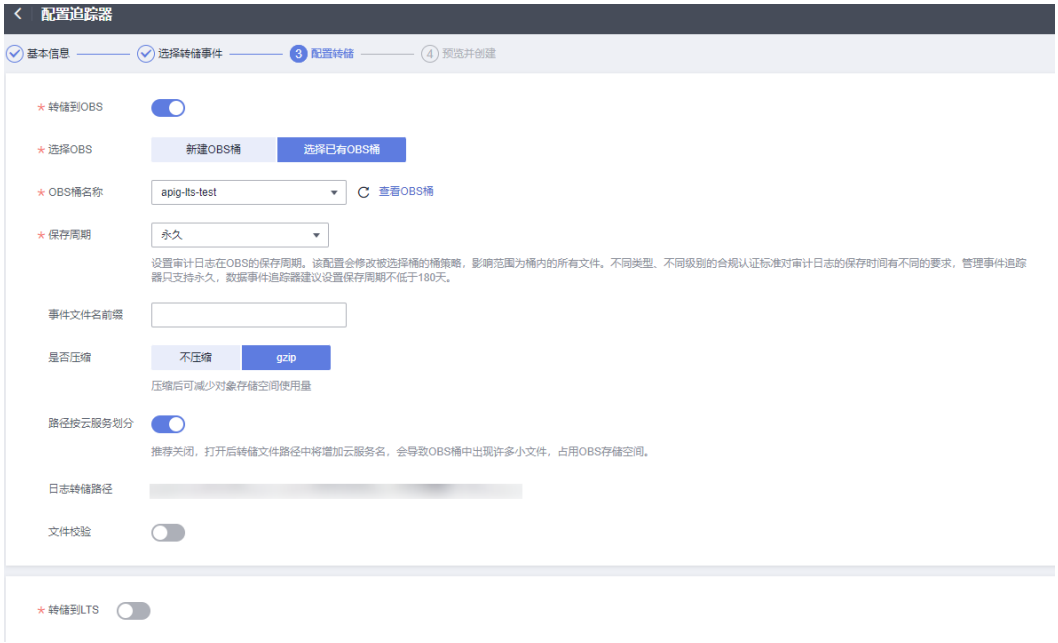
图 2-1 事件列表



2.2 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KMS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**。

图 2-2 配置转储



2.3 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 2-3 关键操作通知

图 2-4 邮件通知

2.4 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**。

2.5 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 2-5 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 2-6 告警策略

2.6 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**。

3 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 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤3 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4 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。
排除KMS事件	默认不勾选。勾选后，追踪器将不会转储用户对数据加密服务（DEW）的相关操作。 **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。

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。

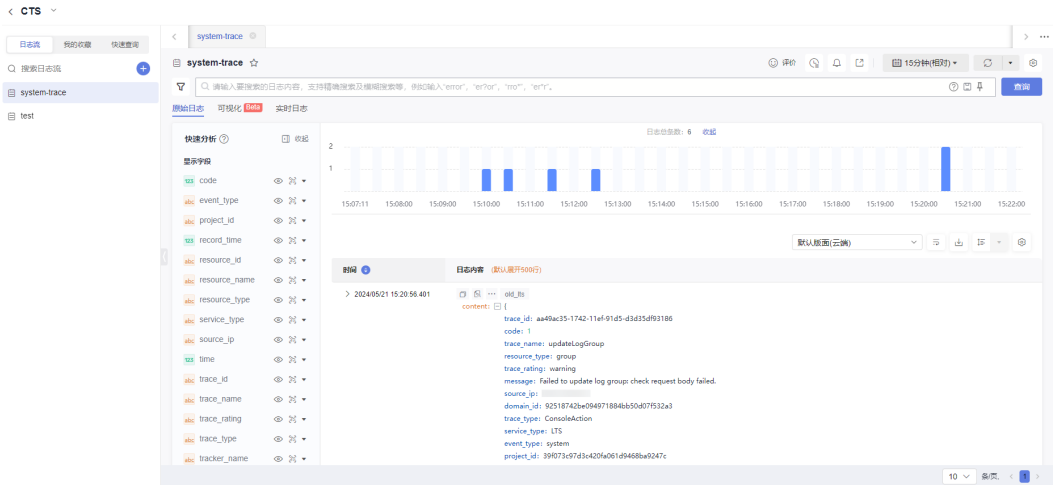
----结束

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。

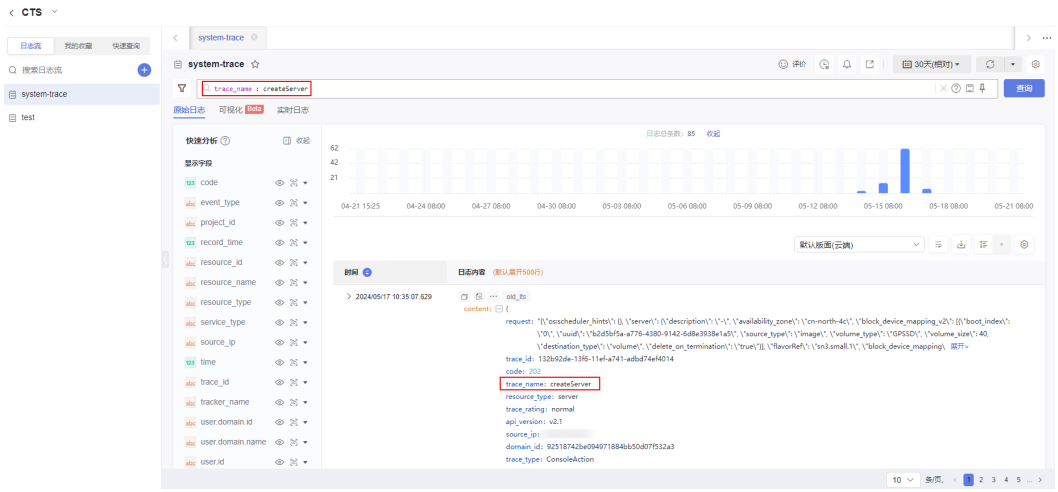
图 3-2 单击日志流名称

图 3-3 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。



----结束

