云审计服务

最佳实践

文档版本01发布日期2025-07-03





版权所有 © 华为云计算技术有限公司 2025。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

NUAWE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: <u>https://www.huaweicloud.com/</u>

1 CTS 最佳实践汇总	1
2 结合函数工作流对登录/登出进行审计分析	3
2.1 案例概述	3
2.2 准备	4
2.3 构建程序	5
2.4 添加事件源	5
2.5 处理结果	6
3 CTS 安全最佳实践	7
3.1 启用云审计服务,便于云上用户对操作的事后审查	7
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	7
3.3 开启云审计服务,请配置审计事件通知	8
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	9
3.5 使用云监控服务对重点审计事件进行实时监控告警	9
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	10
4 通过云日志服务 LTS 存储和查询审计事件	11
5 使用云审计服务监控"创建 IAM 用户"操作	14
6 使用云审计服务监控 AccessKey 的使用	18
7 使用云审计服务监控华为云账号的使用	23
8 下载云审计服务记录的操作事件	27
9 通过云审计服务监控 DEW 密钥的使用	29
10 将云审计记录的事件持续投递到指定服务	32
11 CTS 安全配置建议	38

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。
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。
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。

最佳实践	说明
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)。
CTS安全配置建议	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。

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<mark>步骤3</mark>;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<mark>给IAM用户授权</mark>。

- **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<mark>支持审计的服务及操作列表</mark>。

----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"。

门 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<mark>示例代码</mark>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<mark>创建委托</mark>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<mark>表2-1</mark>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<mark>准备</mark>中开通的CTS云审计服务,创建CTS触发器,CTS触发器配置如<mark>图2-2</mark>所示。

文档版本 01 (2025-07-03)

图 2-2 创建 CTS 触发器

创建触发器

触发器类型 ⑦	云审计服务 (CTS)	~	•		
	可以编写FunctionGraph函数 务获取已订阅的操作记录后, 数。 一个Project下CTS触发器可能	X,根据CTS云审计服务类型和 通过CTS触发器将采集到的描 创建数最多10个,现已创建2个	操作订阅所需要的 操作记录作为参数传	事件通知,当CTS云审 ·递来调用FunctionGra	ì计服 ph函
	⊘ 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、数字和下均	划线, 且长度不能超过64个字节	ŧ.		
白定义操作	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	ſſE
	IAM 🗸	user X V	login × logout ×	~	除
	添加自定义操作				

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<mark>图2-3</mark>所示。

图 2-3 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<mark>责任共担</mark>。

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,更好地组合使用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<mark>开通云审计</mark>。

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

事件列表 ③							[2] 使用指引 〇> 返回旧板
(THE V							
最近1小时	~	Q 选择届性筛选,或输入关键字搜索	事件名称				Q
事件名称	云服飾	资源类型	资源名称	资源ID	操作用户	事件报别	操作时间
login	IAM	user		ba24ccefcfd3492f924eb45e0c		o normal	2024/07/17 14:30:24 GMT+08
loginFailed	IAM	user	Itstest	5a0215bed7a14de38193a6749	Itstest	 warning 	2024/07/17 14:24:36 GMT+08
login	IAM	user	Itstest	5a0215bed7a14de38193a6749	Itstest	o normal	2024/07/17 14:05:25 GMT+08

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

< 配置追踪器	⑦基本思想 — 2 REMAR) 形成并创建
云审计服务基础功能先	頃、専4分析、CBS的体況共識型作者辺可能が生少信息時、具体現所自己IS、CES、CENVESMANd間、了解集所型性別計算に指	
转储到OBS 🔵		
 创建云服务委托 创建追踪器时, 	7. 贡献计概装符合思动发现——个元期系编行。cbu_adomibuck	
* OBS稿所雇用户 ⑦	<u> 当前两户</u> 其也而户	
* 🖂 🗷	44.47 回 ∨	
★ 透揮OBS	制造OSSI将 是IRED/ODSI将	
* OBS橋名称	attach-data-buokar-01 v Q 意思OSES第 C	
保存周期	Jimoesam ·	
	企業新日告在G6898月7月期,該監護会使改建品得輸的機能。影楽活躍3時的対所和文件,不同與型。不同原型的合規以正応型方容日告出時行行時有不同的意义。管理導作語時間行及均G8型置(同和文化的主命期期期間使用容在G68的監選、CTS不会使為),數据導作語序置違い 第74任子180天。	注重保存两
事件文件名前缀	bj4	
	月経治療法学毎、数字、下経経(二)、中地経(二)、小教会(二)組織。	
是否压缩	不旺於 9年	
	因集印可心力集件检查问使用量	
路径接云报师划分		
	推荐为55、17开后时4篇公中将徽加三层版名名,会导取6884年出版许多小文件,占用688574条之间。	
日志時儲路径	affaci-data-bucker/01/CloudFracesion-exet%-4202407/17/hystem/安陽祭向4_000K joon.gz	

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

< 创建关键操作	通知
基本信息 通知高校	ispOpenie_PPo_20my 最大化中容的、发展中区、规定、数学板下石刻低。
配置操作 适中的操作将作为制 操作类型	2018、こ前小2014月1、1月17日201400000000000000000000000000000000000
BRNIS ()	
配置用户 当指定的用户发起关 指定用户	#約6月7,可以選邦者はSAN+通知信用 7月82 1002
用户列表	AWER-MI, BEWIELMARA
配置SMN主题 发送通知	*Fau 223

图 3-4 邮件通知

38 PAOL 2
###ロッチンスス用デー pads aphil_2004160/0211
深的资源 ydstest 在 ECS 服务于 2022-12-09 05.52.45 GM1+0.500 发生创建操作, 请念大注: 评见 <u>太中日服务</u>
区域: 马三张也-二条二
操作事件: createServer
操作对象: ECS(ydstest, daeb36ae-f43e-445b-9ff4-221fb16654fc)// 服务名称(资源名称, 资源 ID)
操作时间: 2022-12-09 05:52:45 GMT+0300
操作租户: kaifatest
操作记录内容:
<pre>[api_version]:[1.0],</pre>
message : success.
project_10 : 284(3300C6896)(10)/30609UDICLET , "record time": 2022-112-09 05:52:45 GMT+0300".
"request":"{"server":{"adminPass":"********","extendparam":{"chargingMode":"0", "regionID":"cn-no
f6938e9617bf\"}","support_auto_recovery":"true"},"count":1,"metadata":{"op_svc_userid":"0d45adbc1480d561
7a, description: ", name: ydstest, imageRef: c5242b93-f182-4dd9-b7f5-
<pre>Isize2c19dc , Foot_volume : { volumetype : bala , extendparam : { resourcespectode : bala , resourcesype large & "nergonality": [] forgid: "11661819-ac46-480b-8b3-720bec42c5b" [security groups": [[fid]: "82cf</pre>
677dadfd7ca9, nictype:: . ip address: . portid :null, binding;profile : [disable_security groups :
ename":false, "server_tags":[], "batch_create_in_multi_az":false, "user_data":""}}",
request_id : null,
resource_ld : daeb3bae=143e=443b=9114=2211b16b341c ,
resource_type : ecs,
"response":"("job_id":"8abf964784d2633f0184f4cc2b3601cc","job_type":"createSingleServer","begin_
09T10:52:45.278Z", "status": "SUCCESS", "error_code":null, "fail_reason":null, "entities": {"server_id": "daeb:
Service_type : BCS,
"time": "2022-12-09 05:52:45 GMT+0300".
"trace_id":"8ecf0b36-776c-11ed-ba77-5dda34f629a2",
"trace_name":"createServer",

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

云监控服务	事件监控 ③					自建吉蓉规则
a控概题 和的看板 NEW	近小时 近3小时 近1	2小时 近24小时 近7天	近30天		<i><u></u></i> <u></u>	第一结末日期 🗒 🗋
1月19日 1月19日	◎ 设置 当前监控数据采用的聚合算法为	"周期:1小时,方法:求和值"。				 系統事件 自定文事件
ER1监控 ~	12					
地议监控	8	•				
102222	4 2					
58中心 《	0 2024/07/16 14:47:56 2024/07/16 16:47:56	2024/07/16 2024/07/16 18/47/56 20/47/56	2024/07/16 2024/07/17 22:47:56 00:47:56	2024/07/17 2024/07/1 02:47:56 04:47:56	7 2024/07/17 2024/07/17 06:47:56 08:47:56	2024/07/17 10:47:56 12:47:56
	〇、选择履性筛选,或输入关键字搜索					
	 ・ ・ ・	事件名称 ⊖ 用户登录	事件来题 ⊖ 统一集份认证服务	事件数量 ⊕ 20	最近发生时间 ⊖ 2024/07/17 14:30:24 GMT+08:00	操作 查看监控图表 创建需要规则
	 	用户登出	统一身份认证服务	29	2024/07/17 12:50:52 GMT+08:00	查看並投限表 创建吉蓉规则
	 £他事件 ¥他事件 	Config快服导出失败 制脉波和机	配置审计 课件云报条器	1	2024/07/17 07:15:24 GMT+08:00 2024/07/16 16:36:39 GMT+08:00	2018年20月末 612年25月月 2019年 612年25月月
	○ 系統事件	BRUE	云硬鱼	1	2024/07/16 16:36:37 GMT+08:00	查看出地研奏 创建常智规则

设置告警策略,可以设置一个事件周期,阀值超过设置可视为此用户登录异常产生。

图 3-6 告警策略

* 告誓策略

事件名称	告誓策略			告警级别 操作
著創物的	~ 在5分钟内	◇ 第计級发 ◇ 1	次 则 毎1天告替次 >	重要 〜 教諭
· 希 修改idp	✓ 在5分钟内	~ (累计触发 ~) 1	次则 每1天集藝—次 >	
著 更新metadata	✓ 茬5分钟内	◇ 第計触波 ◇ 1	次则 每1天告誓 次 >	
晋 更新张导型录策略	~ 在5分钟内	× 第計税税 × 1	次则 每1天告誓 次 >	
著创建AK/SK	~	観没 1	次 则 舌髎—次	重要 〜 影除

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<mark>开通云审计服务</mark>。

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

云审计服务	追踪器 ③											
事件列表	● C15003股7天約3個作單4: 想要要创建色好線长保存提长打包的單4、面包体充出進度7天前約個作單4, 通路操会件要付款機保存分回機但A15日目式成素068時中。											
10.15H	868											
学编辑化最初 想还可以创建99个数据通时题。0个管理组制题。												
	○ 法释雇性筛选,成	意入关键字搜索追踪器名称								00		
	16151824 O	秋志 〇	甲件类型 ⊖	是否开通组织	追踪对象 0	存储服务 🖯	1625 O	企业项目 ↔	900906 0	操作		
	system	0 正常	◎ 管理事件	8	-	OBS smjtest 🗹 LTS CTS/system-trace 🕑		default	2023/08/08 19	配置 動除 停用		

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。	default
	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 <mark>创建企业项目</mark> 。	
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。	不勾选
	况明 数据加密服务(DEW)的相关审计操作请参考 <mark>数据加密服务相关</mark> 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。

I	图 4-2 开启转储到 LTS 功能									
	< 配置追踪器		○ 基本信息 ————————————————————————————————————	2 02384968	- (3) \$%5#61\$					
	1 云审计报册基础功能免费	1. WH2HF. 085H4時代が建築の後に生まり最高年、単に意味色はTS, 085, DEWESMW6員、7所高市所自治H書が同じ								
	转储到OBS 🔵									
	转储到LTS * 日志派名称	(CTS) BATWATHABICTSynam fan (Cleino, Honallent, Marsadrallentweis, Ingwebsolumm,								

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

五甲川服 另	追踪器 ③									OR PROPERTY AND IN THE PROPERTY AND INTERPOPERTY AND INT)
事件列表	 CTS仅记录7天内的部 	L作事件,它需要创建违称器	来保存更长时间的事件,否则将引	6法追溯7天前的操作事件,追踪	家議会将事件持续保存到您预定	的LTS日志流成者OBS稿中。					
追踪器											
关键操作进知	您还可以创建99个数据3	1時間、0个管理追時間。									
	Q 选择屬性筛选,或	输入关键字搜索追踪器名称								00	
	1253838 O	¥62 ⊖	事件类型 ⊖	是否开通组织	出版对象 0	存保服务 ⊖	毎盆 8	<u>企业项目</u> ⊖	98201A 0	操作	
	system	0 正電	◎ 管理事件	8	-	OBS smitest 🗹		default	2023/08/08 19	10.00 Bills (978	

图 4-4 system-trace 日志流页面

< CTS ~								
日本流 死的攻藏 快速面洞	< system-trace ©							
Q. 搜索日志流	⊜ system-trace ☆						0 ## C L L	(自 30天(相対) *) (ジー・)
system-trace	♀ Q 清喻入要推想	的日志内容,支持	持精确搜索及横相搜索等,例如输入	"error", "er?or", "rro"", "er"r",				0 🗆 4
iest	日志複索 日志分析	eta 搜索分析	Beta 实时日志					
	快速分析 ②	- 818	1.3К		日志	·····································		
	显示字段 123 code	© % •	862 ··· ··· ··· ··· ··· ··· ··· ··· ··· ·					
	ac event_type	◎ ≥ •	06-17 15:56	06-23 08:00	06-28 08:00	07-03 08:00	07-08 08:00	07-13 08:00
	abc project_id	© % •						
	123 record_time	© X •					默认版面(云鏡)	> 2 ₹ 15 .
	<pre>icc resource_idicc resource_name</pre>	© X • © X •	11日 🖯	日志内容 (武以展开500行)				
	acc resource_type	⊚ ≥ •	> 2024/07/17 15:26:37.572	C R ··· old_its				
	acc service_type	• × •		trace_id: e7341	b12-440d-11ef-bd45-db1f6d2dc5	ic7		
	abc source_ip	© % •		code: 1 trace_name: up	idateLogGroup			
	123 time	© × •		resource_type: trace_ration:_w	group			
	abc trace_id	• % •		message: Faile	d to update log group: check requ	est body failed.		
	abc tracker_name	© × •		source_ip: domain_id: 925	18742be094971884bb50d07f532a	a3		
	atc user.domain.id	© % •		trace_type: Cor service_type: 1	nsoleAction rs			
	abc user.domain.nar	te ⊚≋ •		event_type: sys	tem			
	abc user.id	© 🐹 🔹		project_id: 39f0	073c97d3c420fa061d9468ba9247c			

- 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

CIS ·								
日志流 我的权能 快速查询	< system-trace ©							
Q. 搜索日志流 🕒	⊜ system-trace ☆							□ (田对) • (① •
system-trace	Trace_name :	treateServer]					× (2) 🛱 🛛 🛤
🗐 test	日志按索 日志分析 🔤	也 搜索分析	Beta 实时日志					
	快速分析 ②				E	1本忠系数:20 次起		
	显示字段		4					
	123 code	⊗ ≥ •	2					
	abs event_type	• % •	05-17 16:02	05-23 08:00	05-28 08:00	07-03 08:00	07-08 08:00	07-13 08:00
	project_id	⊗ ≥ •						
	123 record_time	• % •					默认版面(云端)	× 5 ± ⊯ • ⊗
	see resource_id	© % •	Big 🕒	日志内容 (默认展开500行)				
	is resource_name	• % •						
	iresource_type	© % •	> 2024/07/12 08:57:25.394	content: - (
	service_type	• % •		request: "(\"ser	ver\":{\"adminPass\":\"********\",	\"extendparam\":{\"chargingMode"	\":\"0\".\"regionID\":\"cn-north-4\").\"	'count\":1,\"metadata\":
	source_ip	© % •		(\ op_ 4g\'',\'	description\"\"\",\"name\"\"ecs	-CDNtest\",\"imageRef\"\\"502bd9	46-6777-47c5-bb4b-a8804bb30596\"	\/"root_volume\ 展开>
	123 time	• × •		trace_id: b4255	599-3fe9-11ef-a6a7-eb50a08500	02e		
	😹 trace_id	© % •		resource_type:	ecs			
	👞 tracker_name	© % •		trace_rating: no api version: 1.0	rmal			
	😹 user.domain.id	© % •		message: succe	55			
	user.domain.name	• * * •		source_ip: domain id: 925	18742be094971884bb50d07f532	2a3		
	user.id	@ % •		trace_type: Cor	soleAction			

----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(华北-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。
- 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"ctstest"),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<mark>产品价格详情</mark>。

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

L

云审计服务	追踪器 ③											
事件列表	❶ CTS仅记录7天内的摄	作事件,您需要创建违踪器。	·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	除器会将事件持续保存到您指定	的LTS日志流或者CBS稀中。						
858												
关键操作通知	您还可以给赚到9个数据通报器。0个答理通报器。											
	〇、法経腸性院法、或は	意入关键字搜索追踪器名称								00		
	1000000 0	秋志 日	●件类型 ⊖	是否开通组织	·追归对象 0	存储服务 🖯	4≅25 ⊖	企业项目 🖯	emenie 0	操作		
	system	0 E%	③ 管理事件	8	-	OBS smjtest C LTS CTS/system-trace C		default	2023/08/08 19	配置 動除 停用		

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

配置操作					
远中的操作将作为雕	逻器,在操作发生时,即时发送SMN通知。				
操作类型 ⑦	完整自定义				
操作列表	请选择服务类型	∨ -请选择资源类型	✓ −请选择!	最作名称	~ 添加
	您可以添加100个服务,1000个操作。了解操作详	青,了解更多 🖸			
	服务类型	资源类型	操作名称	操作	
	IAM	user	createUser	删除	
高级筛选 ⑦					
配置用尸 当指定的用户发起关	·腱擾作时,可以选择通过SMN通知相关的订阅者。				
指定用户 곗	不指定 指定				
用户列表	不指定用户时,则默认指定所有用户。				
配置SMN主题					
发送通知 ⑦	不发送发送				
	 ● 創建云設务委托 ● 創建关键操作通知时,云审计服务将至 	:自动创建一个云服务委托:cts_admin_trust			
SMN主题	cts-test	◇ 创建主題 2			

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 成功接收到"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。

204	(約) 化为云田户					
	(約)深语 tert 在 IAM 服件工 2024 10 29 17:2	2:44 GMT+0900 学生协作 速位注				
	1245514 (44) 北京町	LITT CHIT COUCH DELERTY, MILES	01. P98 <u>24011809</u>			
	操作+wiff: createUser		-			
	操作对象: IAM(test, 4tcb	09da)// 服务名称(资源名	标, 资源 ID)			
	操作时间: 2024-10-29 17:32:44 GMT+0800					
	操作用户:					
	操作记录内容:					
{						
	"code":201,					
	"domain_id":"7e0di	7cba",				
	"operation_id":"KeystoneCreateUser",					
	"project_id":"0706	286e",				
	"read_only":false,					
	"record_time": 2024-10-29 17:32:44 GMT	+0800",				
_L	equest":"{"user":{"domain_id":"7e0d	7cba", "pwd_statu	is":false, xuser_id":"", name":"test", mobile	":", "xuserId":", "description":", group	os":[], "xuser_type":"", "access_mode":")	programmatic", em
	resource_account_id : /eUd	/cba ,				
	resource_1d : 41cb	U9da ,				
	resource_name . test ,					
	"service_type": "TAM"					
	"source ip": "124, 71, 93, 164".					
	"time":"2024-10-29 17:32:44 GMT+0800",					
	"trace_id":"c0453409-95d8-11ef-827a-4b	ua7d5c48b93″,				
	"trace_name":"createUser",					
	"trace_rating":"normal",					
	"trace_type":"ConsoleAction",					
ินธ	er":"{"access_key_id":"HS 4Y	/", "account_id": 7e0d	7cba", "domain": {"id": "7e0d	7cba", "name":"	"}, "id":"#369	1214", "name"
1	"user_agent": Mozilla/5.0 (Windows NI	10.0; Win64; x64) AppleWebKit/5	37.36 (KHIML, like Gecko) Chrome/117.0.0.0 Sa	fari/537.36		
) mt23						
1250	840/314F/37C037C14:					

----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(Access Key ID)和访问密钥密码(Secret Access Key),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<mark>产品价</mark> 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

云审计服务	追踪器 ③								SIES
事件列表	● CTS仅记录7天内的操作	1事件,您需要创建违踪器	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	3器会将事件持续保存到您 描定	的LTS日志流或者CBS稿中。			
10.178									
关键操作通知	您还可以创建99个数据追	珍臻,0个管理追珍器。							
	Q 法释题性知法,或M	前入关键字搜索追踪器名称							00
	SFBSR 0	秋恋 ⊖	●件类型 ⊖	是否开递组织	16.1675 ()	存储服务 🖯	1ā35 ⊖ ú	· · · · · · · · · · · · · · · · · · ·	间 操作
	system	O ER	◎ 管理事件	8	-	OBS smjtest 🗹	d	efault 2023/0	8/08 19 配置 動態 停用

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

< 配置追踪器		○ 羅本信息 ——	— (2) RE3184948	— (3) 17:15#01 8
① 云审计服务基础功能免	8. 事件分析、GesH编码关键最优图成问题产生少量最高,具在最后面15、Ges、DEWKOSMW8篇,了就最后数位用计数评值 🖸			
\$\$推到OBS ①				
转编到LTS				
*日志紹名称				
	编作事件特殊通到CTSWystem-trace 已日志运中,诸勿向该日忠远可入罪他数据或导致日忠远相关和量,否则可能导致部分功能得常。			

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

云审计服务	追踪器 ③									962557 8
事件列表	❶ CTS仅记录7天内的操作	1事件,您需要创建追踪器	味保存更长时间的事件, 否则将列	已法追溯7天前的操作事件,追踪	家聯合将事件持续保存到您預定	的LTS日志流成者OBS稿中。				
关键操作通知	您还可以创建99个数据是 〇 洗程展件装洗、或	5日,0个管理自行器。 1入关键字搜索消防器名称								
	ARMER O	秋志 ⊖	事件类型 ⊖	星否开通组织	215712 O	存储服务 〇	65盆 ⊖	£± ₩ÿEI 0	eleberia o	###
	system	 正常 	◎ 管理事件	ē	-	OBS smitest 🗹		default	2023/08/08 19	1018 1019 (FR

图 6-4 system-trace 日志流页面

(CIS								
日本流 我的欢迎 快速重调	< system-trace ©							>
Q 接來日志流 🕀	⊜ system-trace ☆						0 ## Q A 12	□ 30天(相対) ▼ ③ ▼ ⑧
system-trace	♀ ○ 通知入臺建築	的日志内容,支持	持续强度及横端强度够,但如输入;	error", "er?or", "rro"", "er"r".				0 🖬 🖡 💼
🗎 test	日志複数 日志分析 🔝	大 日志分析 (Bata 抱紫分析 (Bata 实时日志						
	快速分析 ⑦ 显示字段		1.3K 862					
	event_type	© X •	06-17 15:56	06-23 08:00	05-28 08:00	07-03 08:00	07-08 08:00	07-13 08:00
	acc project_id	© X • © X •					默认版面(云論)	- 5 b H + 0
	atc resource_name atc resource_type	© X • © X • © X •	H161 ● > 2024/07/17 15:26:37:572	日石内容 (秋以東开500行)				
	atc service_type	© X • © X •		trace_id: e7341 code: 1 trace_name: up resource_type:	b12-440d-11ef-bd45-db1f6d2dc5 dateLogGroup group	c7		
	es trace_id	0 X * 0 X * 0 X *		trace_rating: w message: Faile source_ip:	aming d to update log group: check requ	est body failed.		
	user.domain.id	0 X +		trace_type: Co service_type: L event_type: sys project id: 39f	1107460800071322 IsoleAction FS tem 173697d3c420fa061d9468ba9247c	10		

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<mark>配置索引</mark>。

图 6-5 搜索 access_key_id

< system-trace •	> •	··· ©
(文語第四) □ ***********************************		80
		_
> 22 2024/12/02 10/22 40 058		
request: "{\"trainer"\"Op-access-keys-rolated"\"state"\"Enabled"\"iAdeCoption\"\'IAdeEngli的接近就是无政力的结构,现为不会成"\"period"\"faveniyFour_Hours\"(parameters)"\ (\"maxAccessKeyJege"\		
("value"1901]).1909pr7joef"10elog1.stoplog_essionment_type"110ultin1.10olog_66Inition_051/ 7ai1/10oman_66111 Itace_61	V}*	
code: 200 bace_nume: createPolcyAssignments		
records_type: policy trace_ration; normal		
ap, versions, V1 source, (or detamation)		
trace_type: ApCall reaction to the control of the c		
event, type: _dobal project, dd:		
	-	
制、規力の合計の「Lineadeal Lineadeal LinearLi	17396	
02T02-23-40 22027(\'policy_definition_jdf\\' \\'parameters?\\'maxAccessKeyAge 展开>		
resource_ld:		
tracker_name: system		
operation_id: CreatePolicyAssignments		
resource_account_id:		
ume: 1/3310022008		
record type (T32) (000 C C C C C C C C C C C C C C C C C		
access key id: HST NDB		
account.id: §		
domain: 😁 []		
name: //ServiceLinkedAgencyForRMSMuttAccountSetup		

步骤4单击搜索框右侧的²²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 创建快速查询 * 快速查询名称 快速查询AccessKeyID * 快速查询语句 access_key_id : HST NDB

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	
< CTS	\sim
日志流快速查询	
请输入快速查询名称	Q
快速查询	~
🖹 system-trace	(1) 🔻
D: 快速查询AccessKeyId	

----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^Q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<mark>产品价</mark> 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

云审计服务	追踪器 ③									siess
事件列表	0 CTS仅记录7天内的描	作事件,您需要创建进踪器	来保存更长时间的事件,否则将矛	E法追溯7天前的操作事件,追踪	3器 会将事件持续保存到您指定	的LTS日志流或者CBS稿中。				
10.15-85										
· 关键操作遭知	您还可以创建99个数据追	診證, 0个管理追踪器。								
	○ 选择履性常选,或制	前入关键字搜索追踪器名称								(a) (a)
	追踪器名称 ⊖	秋志 Θ	●件类型 ⊖	是否开通组织	追踪对象 ()	存储服务 🖯	4≅25 ⊖	企业项目 🖯	eneenii o	操作
	system	 正常 	⑥ 管理事件	8	-	OBS smjtest 🗹		default	2023/08/08 19	配置 影除 停用

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。	default
	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 <mark>创建企业项目</mark> 。	
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。	不勾选
	说明 数据加密服务(DEW)的相关审计操作请参考 <mark>数据加密服务相关</mark> <mark>的操作事件</mark> 。	

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

く 配置追踪器		◎ 羅本信思	- (2) Aliateta (3) Misheila
① 云审计服务基础功能免3	8、事件分析、D6SH指体闪光建造作意识可能产生少量意用、具体意思带出了S、D6S、DETYRDSWN编算、了KallERY的提升意识的 🕐		
转储到OBS			
转储到LTS			
* 日志組名称	CT3 MATHANANTENyAMPARA (CB1550), 新加州自己出版列, JAON SAGARD 日出版和关系, 古教可能的数据分为能用用,		

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

云审计服务	追踪器 ③									COLUMN
事件列表 1987年1月	❶ CTS仅记录7天内的操	作事件,您需要创建违踪器	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,进展	家議会將事件持续保存到您預定	的LTS日志流或者OBS稿中。				
关键操作通知		時間、0个管理自時間。 6) - Yestersinに現また。								
	BREAT 0	- K 2 0	事件类型 ⊖	是否开通组织	111111111111	石硝酸焦 🖯	伝道 Θ	企业 项目 ↔	eneenii 0	(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(
	system	0 正常	◎ 管理事件	8		OBS smitest 🗹		default	2023/08/08 19	638 899 978

图 7-4 system-trace 日志流页面

C CIS									
日本流 我的改善 快速重调	< system-trace ©							>	
Q 接续日志流 🔠	🗏 system-trace 🏠						0## Q D D	(目 30天(間対)・) (ジー・)	
system-trace	▼ Q 導輸入業提供的日志内容,支持導端提供及機構提供等,例如輸入*error', 'er?or', 'ror'', 'ror'', 'er?r'.						0 II 4		
😑 test	日志独宏 日志分析 😢	18 搜索分析							
	快速分析 ⑦ 显示字段	i 838	1.3K 862 431		Ba	自然数: 5,501 (722)			
	event_type	* X *	06-17 15:56	06+23 08:00	05-28 08:00	07-03 08:00	07-08 08:00	07-13 OB:00	
	sec project_id	© % * © % *					默认版面(云纳)	~ 5 H H + ®	
	<pre>we resource_id we resource_name</pre>	© X • © X •	81A 🖨	日志内容 (取り取开500行)					
	<pre>web resource_type web service_type</pre>	 ○ × • ○ × • 	> 2024/07/17 15:26:37:572	content: - { trace_id: e7341	b12-440d-11ef-bd45-db1f6d2dc5c	c7			
	source_ip	 ○ × • ○ × • 		code: 1 trace_name: up resource_type:	dateLogGroup group				
	trace_id	race_id ⊚ ∺ -		trace_rating: warning message: Failed to update log group: check request body failed. source_jp:					
	acc user.domain.id	© X •		domain_id: 925 trace_type: Cor service_type: U	18742be094971884bb50d07f532a isoleAction 'S	13			
	atec user.domain.nam	• © × • © × •		event_type: sys project_id: 39f0	tem /73c97d3c420fa061d9468ba9247c				

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。
- *{usernamej*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"。

API凭证 ③	
● 有关华为云账号,IAM子用户和项目的相关信息,请点击这里	
IAM用户名	账号名
「D Dinh用用MAI	Ci di Billiona di

图 7-5 搜索 user.name

<	syst	tem-trace ©				> … @
(交互機対	t user.name:	aomtest			
	abc proy	ect_id ⊚≋, ▼				
	123 reco	ord time 🐵 🕱 🕶	时间 🔶	日志内容 (武以展开500行)		8
	abc reso	ource_id @ 😭 🕶	> 1 2024/12/03 15:12:45.613	C old_lts content: □ {		
	abc reso	ource_n@ 🚉 👻		trace_id:		
	abc reso	ource_t (©)33 •		code: 302 trace_name: login		
	abc serv	vice type 🐵 🕱 💌		resource_type: user		
	abc SOUI	rce_ip ⊚ ≋ •		trace_rating: normal message: "("login\".("model".\"password\",\"us	er_type\":\"iam.user\",\"login_protect\":(\"status\":\"off\")})"	
	123 time	• • × •		source_lp:		
				domain_id:		
	abc trao	e_id ⊚ ﷺ •		trace_type: ConsoleAction		
	abc traci	ker_na 💿 🎉 💌		event type: dobal		
	1100	rdomai do S =		project_id:		
	apc Gard	1.00mail		read_only: faise		
	abc USEI	r.domai 🐵 💢 💌		resource_id:		
	abe USE	r.id 💿 🔍 🔻		tracker_name: system		
				time: 1733209965613		
	abc USEI	r.name 💿 🎘 🔻		resource_name: aomtest		
	abc Cate	egory 💿 😫 💌		record_time: 1/33209965613		
	0.81210			domain: (=) {}		
	abe trace	e_name 🗞 🎘 🔹		name: aomtest		
	trac	e ration 20 92 •		}		
	and trace	~_runny (2/ 24) *		}		
	_{abc} trace	e_type 🗞 🛱 🔹		code: 302 event_type: global project_id:	record_time: 1733209965613 resource_id:	resource_name: aomtest resource_type: user
				service_type: IAM source_tp: time: 17332	19965613 trace_id: tracker	name: system user.domain.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 7-6 创建快速查询 创建快速查询		
★ 快速查询名称		
快速查询UserName	0	
★ 快速查询语句		
user.name : aomtest		

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。

< CTS		~
日志流	快速查询	
请输入快速查	Q	
快速查询		~
🗎 system-tr	(1) 🔻	
Ca 快速查询	UserName	

----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⁴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<mark>配置日志告</mark> <mark>警规则</mark>。
 - 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

- 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<mark>产品价格</mark> 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

云审计服务	追踪器 ③									and the second s	
事件列表 追踪器	● CTS仪记录7天内的操作	(TSI公司教子方式操作事件,总需要会建造到解并用我使更长对我们要并,面包持无法追加了事件,追到最会将事件特殊保持到这编绘的LTSI已去完成者(BSI所作,									
关键操作通知	您还可以创建100个数据追 〇、选择履性描述,或制	段間,0个管理追踪器。 1入关键字搜索追踪器名称								00	
	追踪器名称 ↔	秋念 0	事件类型 ⊖	是否开通组织	BERNE O	存储服务 🖯	标签 ⊖	企业项目 ↔	创建时间 ⊖	操作	
	system	○ 正常	③ 管理事件	2	-	OBS system-bucket-01 🕑]	default	2023/11/03 09:	配置 删除 使用	

- 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

云审计服务	追踪器 ①									0138107595
事件列表	CTS仅记录7天内的编	作事件,您需要创建追踪数	*保存重长时间的事件,否则将7	法追溯7天前的操作事件。追加	家都会将事件持续保存到您指示	的LTS日本流或者OBS橋中。				
10.000										
关键操作通知	想还可以创建100个数据	8時間,0个管理8時間。 輸入关键字提紧追踪器名称								Q
	追踪器名称 ⊖	秋志 0	事件类型 ⊖	是否开避组织	追踪对象 ⊖	存储服务 0	禄签 ⊖	企业项目 ↔	创建时间 🖯	操作
	system	○ 正常	 管理事件 	ă		LTS CTS/system-trace [ð	default	2023/11/03 09:	配置 删除 停用

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

云审计服务	追踪器 ③									62558	
事件列表	❶ CTS仅记录7天内的编	● CT00以已除天外的组件事件, 也需要多值虚与结果有容易长时间的事件, 而到外无法出意开关的的组件事件, 出版器会件事件特殊信件的时间定地以T6日世代成素060纬年。									
10.578											
关键操作遭知	您还可以创建99个数据追问	珍麗,0个管理追珍麗。									
	Q 选择漏性常选,成M	Q. 医希腊性沟压, 前面入头健于建立的方器合称 ② Q ③									
	追踪器名称 🖯	秋恋 ⊖	●件类型 ⊖	是否开递组织	追踪对象 🖯	存储服务 🖯	标器 ⊖	企业项目 ⊖	entenne o	操作	
	system	O 正常	◎ 管理事件	8	-	OBS smjtest 🗹 LTS CTS/system-trace 🖄		default	2023/08/08 19	配置 影除 停用	

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。

○ 云服务: DEW × 资源类型: cmk × 事件名称: scheduleKeyDeletion × 添加筛选条件

○ 云服务: DEW × 资源类型: cmk × 事件名称: enableKey × 添加筛选条件

○ 云服务: DEW × 资源类型: cmk × 事件名称: disableKey × 添加筛选条件

- 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"。
 ① 定錄: DEW × 透調器: cmk × 專件名称: createKey × 述证语语称 × ※
 - 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}"。

Q 資源D: 13a4 5504 × 添加端透影件 × ⑧

🛄 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

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<mark>产品</mark> 价格详情。
- 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(华北-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<mark>约束与限制</mark>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"。

文档版本 01 (2025-07-03)

图 10-1 配置 system 追踪器

云审计服务	追踪器 ①									
事件列表	① CTSC记录为天元如操作等点。如果要创建和后期未保存要长约相处等点。因为并无法通道下关机如晶作等点。通道器会将要将自动成开开到边面当现TS日由流远着005%中。									
1619 2										
关键操作通知	您还可以创建100个数据	自踪器,0个管理追踪器 。								
	(2) 長用層性系统, 認知人又親子我家族局部客称 (3) (3)									
	追踪器名称 ⊖	802 ⊖	事件类型 ⊖	是否开遗组织	過路対象 ⊖	存储服务 ⊖	緑滋 ⊖	企业项目 0	创建时间 🖯	操作
	system	○ 正常	③ 管理事件	ALC: NO	-			default	2019/08/05 14:23:39	配置 動除 停用

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 <mark>组织追踪器</mark> 。 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 <mark>数据加密服务</mark> 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地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 <mark>跨租户转储授权</mark> 。	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 "mybucket"和"mybucket"),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。	FilePrefix
	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	
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。	不开启开 关
	事件文件完整性校验详细操作请参考 <mark>事件文件完整性校验</mark> 。	
	有关摘要文件的更多信息,请参阅 <mark>摘要文件</mark> 。	
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。	不开启开 关
	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。	

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

云审计服务	通踪器 ①									01000000
事件列表 边际器	● C150记表》天内的通行事件、認識者者加減品存錄素符符長於均能的事件、直到件无於追溯的天前的通行事件、適時錄合件事件的条件符約回指是並L15日本洗成者の65%年中、									
关键操作通知	127031110/125555.0/125555. (3.2552/125555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/1255555.00) (3.2552/12555555.00) (3.2552/125555555.00) (3.2552/1255555555555555555555555555555555									00
	追踪器名称 🖯	秋窓 ⊖	事件类型 ⊖	是否开遭组织	出版对象 🖯	存储服务 🖯	标签 ⊖	企业项目 ↔	ଶାହାରାଇ ⇔	操作
	system	O 正常	◎ 管理事件	8	-	OBS system-bucket-0	12	default	2023/11/03 09:	配置 勤除 使用

----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

云审计服务	追踪器 ⊙									estores	
事件列表	● CTSG2是約7元为23個作業4: 認識養金融業務務務務務務										
追踪器											
关键操作通知 您还可以总理100个效振曲频器。0个管理思频器。											
	(C)										
	追踪器名称 ⊖	102 ⊖	事件类型 ⊖	是否开遭组织	追取对象 🖯	transs ⊖	報签⊖	金业项目 ⊖	enerrie o	操作	
	system	○ 正常	◎ 管理事件	香				default	2019/08/05 14:23:39	配置 翻除 停用	

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"。

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 <mark>数据加密服务</mark> 相关的操作事件。	不勾选 "排除 DEW事 件"

表 10-3 设置基本信息

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地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。	СТЅ

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

云审计服务	追踪 器 ⊙									
事件列表	CTS仪记录7天内的模	·春件、忽察要创建追踪器	来保存更长时间的事件,否则将天	法追溯7天前的操作事件。追逐	2000年1月1日1日1月1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1	BYLTS日志流或者OBS橋中。				
追辞器										
关键操作通知	地班可以由國100个数國目	時間、0个管理追踪器。								
	○ 19/2/10/2015/06/00 (○) (○)									
	追踪器名称 ↔	秋志 0	事件类型 ⊖	是否开遵组织	追踪对象 🖯	存储服务 🖯	4≅ 3 0	企业项目 ↔		操作
	system	○ 正常	② 管理事件	M		LTS CTS/system-trace 🕑		default	2023/11/03 09:	配置 删除 停用

-----结束

11 CTS 安全配置建议

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,您需要合理使用云服务提供的安全能力对数据进行保护,安全地使用云。详 情请参见<mark>责任共担</mark>。

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的安全状态,更好地组合使用CTS提供 的多种安全能力,提高对CTS的整体安全防御能力,保护存储在CTS中的数据不泄露、 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。

- 建议妥善管理身份认证信息,减小因凭证泄露导致的数据泄露风险
- 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,提高访问控制
- 开启云审计服务,配置关键操作通知
- 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
- 使用云监控服务对重点审计事件进行实时监控告警
- 开启云审计服务配置OBS桶,将审计事件归档OBS永久存储,并使用DEW对事件 文件进行加密

建议妥善管理身份认证信息,减小因凭证泄露导致的数据泄露风险

无论用户通过CTS控制台还是API、SDK访问CTS,都会要求访问请求方出示身份凭证, 并进行身份合法性校验,同时提供登录保护和登录验证策略加固身份认证安全。CTS服 务基于统一身份认证服务(Identity and Access Management, IAM),支持三种身 份认证方式:用户名密码、访问密钥、临时访问密钥。同时还提供<mark>登录保护及登录验 证策略</mark>。

1. 建议使用临时AK/SK进行业务处理,减小凭证泄露导致您数据泄露的风险

操作CTS相关资源时,都需要进行身份凭证认证,用于确保请求的机密性、完整性 和请求者身份的正确性。建议您为应用程序或服务配置IAM委托或临时AK/SK,通 过IAM委托可以获取一组临时AK/SK,临时AK/SK到期自动过期失效,可以有效降 低凭证泄露造成的数据泄露风险。详情请参见<mark>临时访问密钥和通过委托获取临时</mark> AK/SK。

2. 定期轮转永久AK/SK减小凭证泄露导致您数据泄露的风险

如果您必须使用永久AK/SK,建议对永久AK/SK进行定期凭证轮转,同时加密存储,避免凭证长期使用过程中预置的明文凭证泄露导致数据泄露。详情请参见<mark>访</mark>问密钥。

3. 定期修改用户名密码,避免弱密码

定期重置密码是提高系统和应用程序安全性的重要措施之一,不仅可以降低密码 泄露的风险,还可以帮助用户满足合规要求,减少内部威胁,提高用户的安全意 识。同时建议您配置密码的复杂度,避免使用弱密码。详情请参见<mark>密码策略</mark>。

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,提高访问控制

如果您需要对企业中的员工设置不同的CTS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(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,可以帮助您安全地控制CTS资源的访问。您可以 通过设置CTS系统权限或者细粒度权限进行权限最小化的安全管控。详情请参见CTS权 限管理。

开启云审计服务,配置关键操作通知

云审计提供了关键操作通知能力,便于用户实时接收重点审计事件通知,详情请参见 创建关键操作通知。

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。

当您对华为云的资源增加删除比较关注时,您可以配置云审计关键操作通知并配置相 应资源的服务类型、资源类型、动作,云审计通过消息通知服务(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)。

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,可以在您使用CTS的过程中对您的数据提供更好的 操作体验和更强的保护。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。详情请参见**CTS SDK**。

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,您可以使用CES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。

开启云审计服务配置 OBS 桶,将审计事件归档 OBS 永久存储,并使用 DEW 对事件 文件进行加密

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转储(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,详细操作请 参见追踪器配置OBS转储。

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**。