云审计服务

产品介绍

文档版本 01

发布日期 2024-11-22

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。

目 录

1 图解云审计服务 1
2 什么是云审计服务 3
3 基本概念 5
4 工作原理 8
5 使用场景 10
6 安全 12
6.1 责任共担 12
6.2 服务的访问控制 13
6.3 数据保护技术 13
6.4 审计与日志 14
6.5 服务韧性 15
6.6 监控安全风险 15
6.7 认证证书 15
6.8 Organizations 可信服务 17
7 计费说明 18
8 权限管理 19
9 约束与限制 25

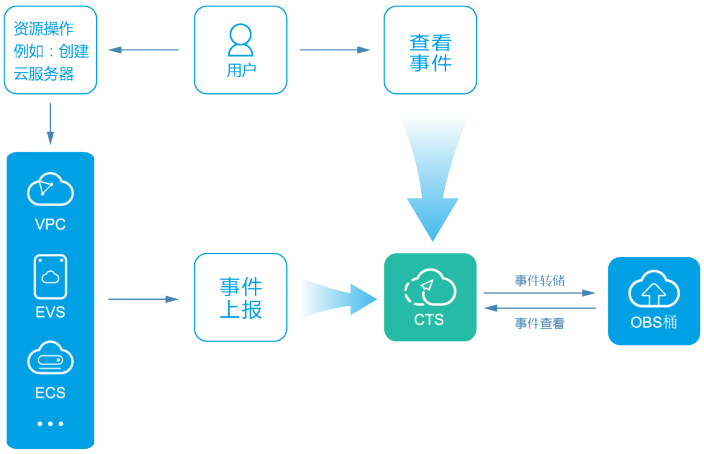
1 图解云审计服务

2 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、问题回溯和问题定位等常见应用场景。

图 2-1 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。

3 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，您也可以在追踪器页面手动创建多个数据追踪器。

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。数据追踪器会记录租户对OBS桶中的数据操作的详细信息。

目前，一个租户仅支持创建1个管理追踪器和100个数据追踪器。

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。

事件分为以下两类：

- 管理事件

  指云服务上报的事件。
- 数据事件

  指OBS服务上报的读写操作事件。

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，包括管理类事件和数据类事件。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。
- 数据类事件指针对OBS桶中的数据的操作日志，例如上传、下载等。

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3-1**所示。

图 3-1 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。

区域

区域指安装云审计服务的服务器所在的物理区域，同一物理区域的可用区之间内网是互通的。

公有云的数据中心分布在全球不同区域（例如，欧洲和亚洲等），通过在不同区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足不同地区的法律或其他要求。

项目

华为云的区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），在区域默认项目中还可以创建子项目，实现更加精细的资源隔离。

4 工作原理

云审计服务直接对接华为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。

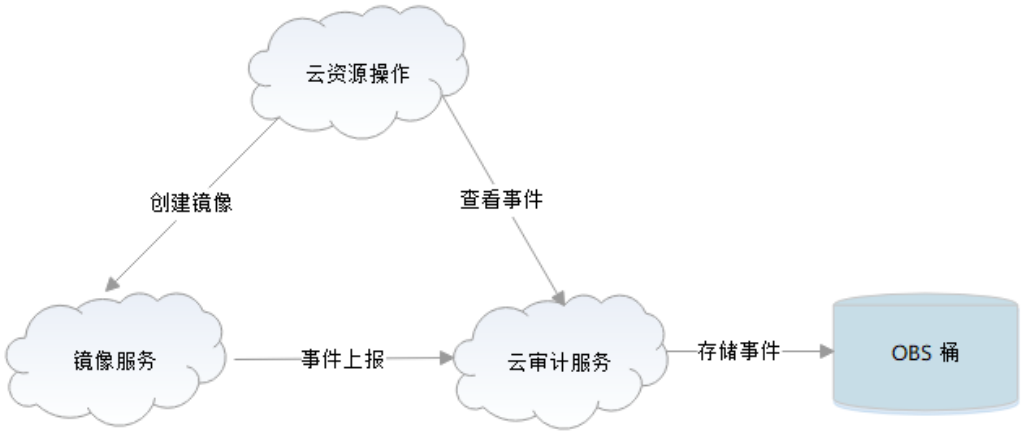
使用云审计服务创建追踪器可以跟踪记录事件文件。如已配置事件转储至OBS服务和LTS服务，事件文件将保存在OBS桶和LTS日志组中。

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。
  - 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，不支持人工删除。
- 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4-1**所示。

图 4-1 云审计服务工作原理示意图



5 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，可以很方便地实现审计类功能，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。

6 安全

6.1 责任共担

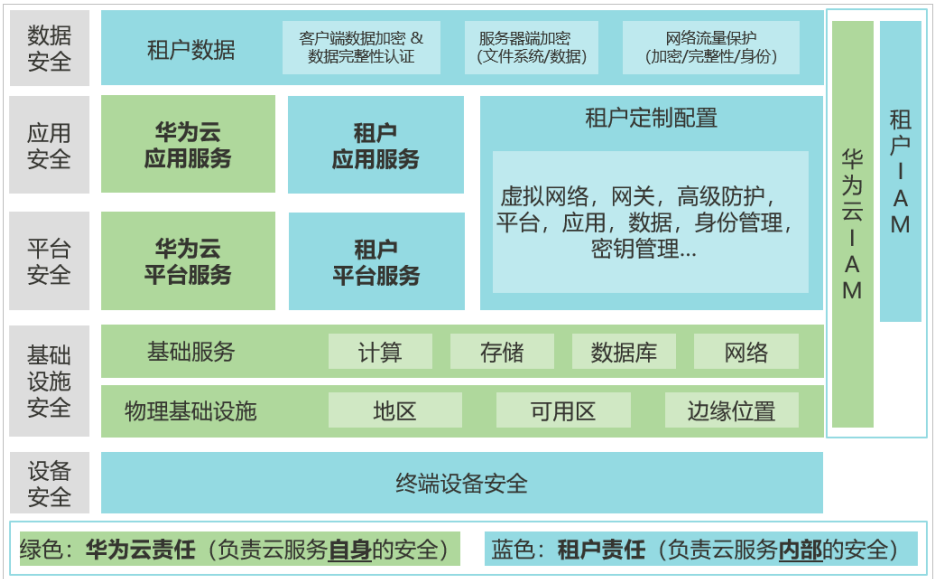
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图6-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 6-1 华为云安全责任共担模型



6.2 服务的访问控制

身份认证

无论用户通过CTS控制台还是API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（IAM），支持三种方式身份认证方式：**用户名密码**、**访问密钥**、**临时访问秘钥**。同时还提供**登录保护**及**登录验证策略**。

访问控制

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，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华为云资源的访问。详细参见**权限管理**。

6.3 数据保护技术

CTS通过多种数据保护手段和特性，保障CTS的数据安全可靠。

表 6-1 CTS 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	CTS支持HTTPS传输协议，保证数据传输的安全性。	**构造请求**
数据冗余存储	审计日志以多副本方式存储，保障数据可靠性。	--

数据保护手段	简要说明	详细介绍
数据转储OBS	CTS支持将日志转储到对象存储服务OBS，并支持转储到加密OBS桶。用户可以以更低成本保存更长时间的日志，同时可以借助OBS的数据保护技术。	创建追踪器
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。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。	开启事件文件完整性校验功能

6.4 审计与日志

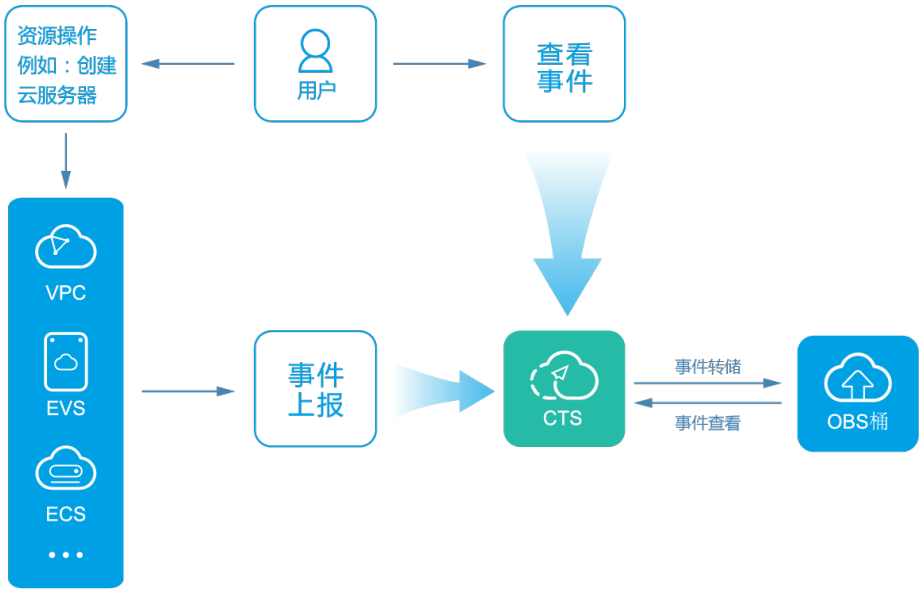
云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户使用云审计服务并创建和配置追踪器后，CTS可记录CTS的管理事件用于审计。

CTS的入门指导和基本操作，请参见云审计服务《快速入门》。

CTS支持追踪的CTS管理事件列表，请参见云审计服务《用户指南》的支持审计的关键操作章节。

图 6-2 云审计服务



6.5 服务韧性

CTS服务提供了3级可靠性架构，通过AZ内实例容灾、双AZ容灾、日志数据多副本技术方案，保障服务的持久性和可靠性。

表 6-2 CTS 服务可靠性架构

可靠性方案	简要说明
AZ内实例容灾	单AZ内，CTS实例通过多实例方式实现实例容灾，快速剔除故障节点，保障CTS实例持续提供服务。
多AZ容灾	CTS支持跨AZ容灾，当一个AZ异常时，不影响CTS实例持续提供服务。
数据容灾	通过日志数据多副本方式实现数据容灾。

6.6 监控安全风险

CTS通过关键操作通知监控安全风险，保障数据安全可靠。

表 6-3 CTS 的监控安全风险

监控安全风险	简要说明	详细介绍
关键操作通知	云审计服务在记录某些特定关键操作时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。	关键操作通知

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行申请下载合规资质证书。

图 6-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-4 资源中心

6.8 Organizations 可信服务

什么是可信服务

组织（以下简称Organizations）云服务为企业用户提供多账号关系的管理能力。Organizations支持用户将多个华为云账号整合到创建的组织中，并可以集中管理组织下的所有账号。用户可以在组织中设置访问策略，帮助用户更好地满足业务的安全性和合规性需求。

可信服务是指可与Organizations服务集成，提供组织级相关能力的华为云服务。管理账号可以在组织中开启某个云服务为可信服务。成为可信服务后，云服务可以获取组织中的组织单元及成员账号信息，并基于此信息提供组织级的管理能力。

云审计服务支持组织云服务的多账号关系的管理能力：

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，组织下所有成员当前区域的审计日志会转储到该追踪器配置的OBS桶或者LTS日志流。

相关链接

什么是组织云服务

什么是可信服务

组织云服务应用场景

组织云服务功能概览

7 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。同时云审计服务与华为云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，数据类追踪器配置的转储事件按照转储的时间保存。
- 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。

8 权限管理

如果您需要对华为云上购买的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华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。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。

如果华为云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是华为云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。由于华为云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8-1所示，包括了CTS的所有系统权限。

表 8-1 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8-2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 8-2 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	√	×	√

细粒度权限说明

使用自定义细粒度策略，请使用管理员用户进入统一身份认证（IAM）服务，按需选择CTS的细粒度权限进行授权操作。CTS细粒度权限说明请参见**表8-3**。

表 8-3 CTS 细粒度权限说明

权限名称	权限描述	权限依赖	应用场景
cts:quota:get	查询租户追踪器配额信息	-	查询租户追踪器配额信息
cts:trace:list	查询审计事件	-	查出系统记录的7天内资源操作记录
cts:trace:listResource		-	
cts:trace:listTraceUser		-	
cts:notification:create	创建关键操作通知	smn:topic:listTopic iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:grantRoleToAgencyOnProject iam:permissions:listRolesForAgencyOnProject iam:projects:listProjects iam:groups:listGroups iam:users:listUsers iam:users:listUsersForGroup	创建关键操作通知
cts:notification:update	修改关键操作通知		修改关键操作通知
cts:notification:delete	删除关键操作通知	-	删除关键操作通知
cts:notification:list	查询所有关键操作通知	-	查询所有关键操作通知

权限名称	权限描述	权限依赖	应用场景
cts:tracker:delete	删除追踪器	-	删除已创建的追踪器

权限名称	权限描述	权限依赖	应用场景
cts:tracker:update	更新追踪器	iam:agencies:listAgencies iam:agencies:createAgency iam:permissions:grantRoleToAgencyOnProject iam:permissions:listRolesForAgencyOnProject iam:projects:listProjects iam:groups:listGroups iam:users:listUsersForGroup lts:topics:list lts:topics:create lts:topics:get lts:logstreams:list lts:groups:get lts:groups:list lts:groups:create obs:bucket:CreateBucket obs:bucket:HeadBucket obs:bucket:GetLifecycleConfiguration obs:bucket:PutLifecycleConfiguration obs:bucket:GetBucketAcl obs:bucket:PutBucketAcl obs:bucket:ListAllMyBuckets kms:cmk:list kms:cmk:get eps:enterpriseProjects:list organizations:trustedServices:list organizations:organizations:get organizations:deletgatedAdministrators:list organizations:accounts:list organizations:deletgatedServices:list	修改已创建追踪器的配置项
cts:tracker:create	创建追踪器		创建一个追踪器用来关联系统记录的所有操作

权限名称	权限描述	权限依赖	应用场景
cts:tracker:list	查询所有追踪器	obs:bucket:GetBucketAcl obs:bucket:ListAllMyBuckets	查看追踪器的详细信息
cts:tag:create	批量添加资源标签	-	批量添加资源标签
cts:tag:delete	批量删除资源标签	-	批量删除资源标签

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**权限及授权项说明**。
- 自定义权限策略具体创建步骤请参见**创建自定义策略**。

相关链接

- **IAM产品介绍**
- **IAM基础概念**
- **创建用户组、用户并授予CTS权限**

9 约束与限制

云审计服务中的追踪器数量和关键操作通知有限定的配额，均不支持修改，云审计服务的具体限制如下。

表 9-1 CTS 约束与限制

限制项	使用限制
一个华为云账号允许创建的追踪器数目	管理追踪器：1个 数据追踪器：100个
一个华为云账号允许配置的关键操作通知数目	100个
一个追踪器允许配置的OBS桶数目	1个
用户操作后多久才能通过控制台查询数据	管理类事件：1分钟 数据类事件：5分钟
组织成员退出组织或被移除组织后，组织追踪器的收回时间	5分钟
用户通过控制台能查询多久的操作事件 **说明** • 云审计默认为每个华为云账号记录最近7天的操作事件，如果不配置转储，您将无法追溯7天以前的操作事件。 • 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，不支持人工删除。	7天
组织追踪器	CTS支持组织追踪器能力，依赖组织服务某些接口，涉及企业项目权限管理的用户如需升级此能力，需要单独配置IAM权限，否则原有仅对CTS:*授权的用户将无法使用组织服务的多账号关系管理能力。

限制项	使用限制
全局级服务需要在中心region（中国-香港）的云审计控制台配置追踪器和关键操作通知，才能使用审计事件上报至CTS功能、审计事件转储至OBS/LTS功能、关键操作消息通知功能。 全局级服务在其他region的云审计控制台配置时，上述功能不会生效。	目前全局级服务包括：IAM、TMS、CDN、DNS、EPS、SMS、SES、SC、cloudsite、CBC、CC、AAD、APIExplorer、DevStarServer、PCA、PSDM、IoTDP、APIErrorCenterService、BSG、ROMAIOC、RMS、IEC、Compass、ExpertCMSService、CSR、ARS、BSS、ExpertCMS、Domains、OSC、Trademark、UCS、IES、CMDB、OSM、SupportPlan、CNAD、GA、TestMind、RAM、Organizations、HMSA、PrivateNumber、VoiceCall、RPM、ICA、EC、OA、marketplacebtm、FunctionFlow、HChatEngineService、HSearchEngineService、APM、MgC、CMN、IdentityCenter、Marketplace、ESM、edgesec、pEDACloud、koopage、OLCS、COST、BILLING、ENTERPRISE、VIAS、CORS、ModernBI、ORGID-MGR、Config、COC、GlobalSIMLink、APIhub、KooPhone、VSS、ACCOUNT、CodeArtsLink、AppStage、HCSS。

