

云监控服务

产品介绍

文档版本 01
发布日期 2023-11-28



版权所有 © 华为技术有限公司 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



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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

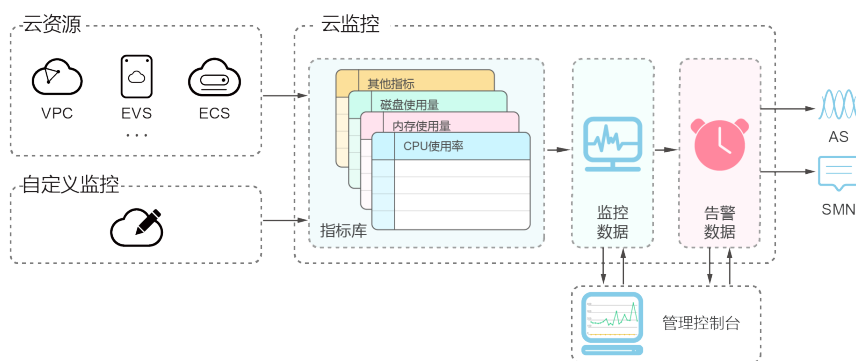
目录

1 什么是云监控服务?	1
2 什么是广域网质量监控?	3
3 服务优势	7
4 应用场景	8
5 服务资费	10
6 云监控服务相关概念	11
7 约束与限制	13
8 安全	14
8.1 责任共担	14
8.2 身份认证与访问控制	15
8.2.1 服务的访问控制	15
8.3 审计与日志	16
8.4 数据保护技术	17
9 区域和可用区	18
10 权限管理	20

1 什么是云监控服务?

云监控服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。云监控服务架构图如图1-1所示。

图 1-1 云监控服务架构图



云监控服务主要具有以下功能：

- **自动监控：**
云监控服务不需要开通，在创建弹性云服务器等资源后监控服务会自动启动，您可以直接到云监控服务查看该资源运行状态并设置告警规则。
- **主机监控：**
通过在弹性云服务器或裸金属服务器中安装云监控服务Agent插件，用户可以实时采集ECS或BMS 1分钟级粒度的监控数据。已上线CPU、内存和磁盘等40余种监控指标。有关主机监控的更多信息，请参阅[主机监控简介](#)。
- **灵活配置告警规则：**
对监控指标设置告警规则时，支持对多个云服务资源同时添加告警规则。告警规则创建完成后，可随时修改告警规则，支持对告警规则进行启用、停止、删除等灵活操作。
- **实时通知：**
通过在告警规则中开启消息通知服务，当云服务的状态变化触发告警规则设置的阈值时，系统通过短信、邮件通知或发送消息至服务器地址等多种方式实时通知用户，让用户能够实时掌握云资源运行状态变化。

- **监控面板:**
为用户提供在一个监控面板跨服务、跨维度查看监控数据，将用户关注的重点服务监控指标集中呈现，既能满足您总览云服务的运行概况，又能满足排查故障时查看监控详情的需求。
- **OBS转储:**
云监控服务各监控指标的原始数据的保留周期为两天，超过保留周期后原始数据将不再保存。您可以在对象存储服务（Object Storage Service，以下简称OBS）创建存储桶，然后将原始数据同步保存至OBS，以保存更长时间。
- **资源分组:**
资源分组支持用户从业务角度集中管理其业务涉及到的弹性云服务器、云硬盘、弹性IP、带宽、数据库等资源。从而按业务来管理不同类型的资源、告警规则、告警记录，可以迅速提升运维效率。
- **站点监控:**
站点监控用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题。
- **日志监控:**
日志监控提供了针对日志内容的实时监控能力。通过云监控服务和云日志服务的结合，用户可以针对日志内容进行监控统计、设置告警规则等操作，降低用户监控日志的运维成本，简化用户使用监控日志的流程。
- **事件监控:**
事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。

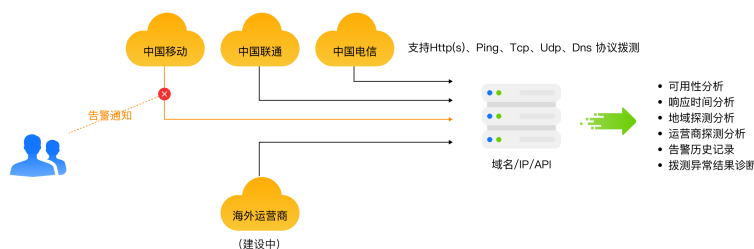
2 什么是广域网质量监控?

概述: 在数字化时代, 网络和服务的稳定性至关重要, 通过拨测功能监控目标对象的可用性, 确保业务稳定运行, 提升企业效率和用户体验。

在数字化浪潮席卷之下, 网络与服务稳定性已成为社会秩序平稳运行的基石。任何网络或服务的突发故障, 深度影响社会的整体运作、企业的持续运营以及民众日常生活的品质, 其所造成的损失往往难以计量。如2022年12月阿里云香港可用区C的服务中断, 故障持续了12个小时以上, 对众多依赖其服务的企业日常运营造成了前所未有的挑战与困扰。

因此, 拨测 (Synthetic Monitoring) 作为网络性能监控中的关键功能, 通过遍布全国的网络探测节点, 模拟用户的实际请求来检测目标服务、DNS或IP地址等对象。这种主动式的网络测试能够监控目标对象在不同地理位置和运营商网络环境下的可用性、性能以及用户体验。利用这一功能, 不仅可以加快故障识别与定位的速度, 还能够帮助企业优化网络资源分配和访问路径, 进而提高整体业务效率和用户满意度。

本文主要介绍拨测的应用场景和主要功能, 更多详细信息请参考华为云云监控的拨测产品: [广域网质量监控](#)。



典型场景

广域网质量监控主要用于模拟真实用户发送对远端服务器的访问, 从而探测远端服务的可用性、网络的连通性等场景。

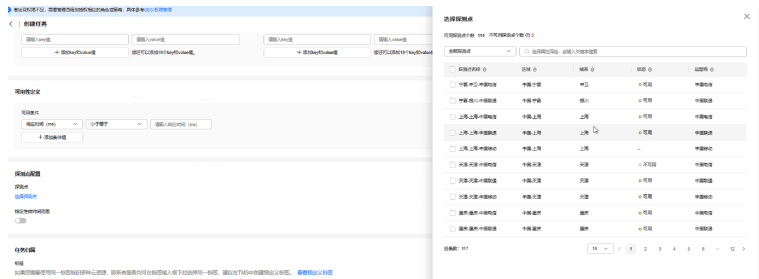
● 场景一: 服务可用性监控

从全国不同城市的运营商节点定期检查网站是否可访问, 以便于提前预警可能影响业务连续性的风险。同时支持用户对探测结果是否“可用”的自定义断言规则, 包含响应延时, 状态码, 响应 body 的内容匹配等。

- **场景二：网络可用性分析**

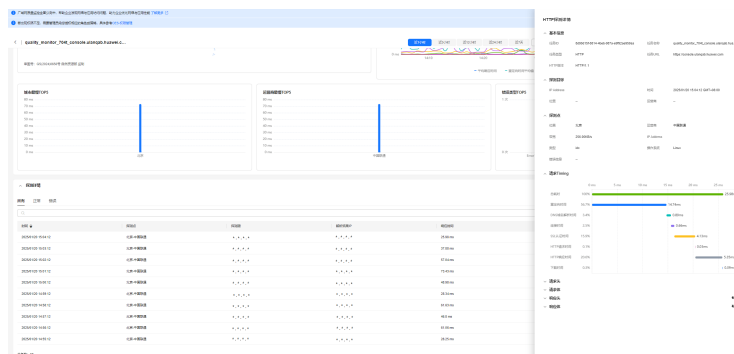
通过使用广域网质量监控功能配置定时PING探测任务，根据需要选择发起探测的不同地域运营商探测节点。（详细请参见：[探测点的分布](#)）

图 2-1 探测点的分布



运行后可以观察到不同地域的运营商线路到目标服务的网络时延情况。帮助决策者制定有效的链路优化和网络产品部署决策，如游戏用户比较关注的运营商链路性能分析等。

图 2-2 探测结果



产品介绍

广域网质量监控通过遍布全国的互联网终端探测节点，发送模拟真实用户访问的探测请求，帮助用户监控全国各省市运营商机房到客户服务站点的网络连通情况。

广域网质量监控归属于华为云监控(CES)，使用广域网质量监控，可免费使用CES的视图、告警模块，与云上资源监控深度融合、打通。通过使用不同的网络层协议模拟用户的在线行为来分析互联网服务和网络的表现，并通过分析延迟、丢包率等关键指标优化用户体验。

- 当前支持的**监控类型**：HTTP、HTTPS、PING、TCP、UDP、DNS。
- 当前支持的**监控指标**：丢包率、响应时间、HTTP响应码、可用性、可用探测点数量、可用探测点百分比。

能力介绍

全方位布局运营商探测点，多元探测按需调控，故障链路可视化呈现，快速定位异常。

- **丰富全面的探测点覆盖**：
全国地域内多个运营商拨测探针发现区域性故障；IDC探测点/家宽PC/手机4G5G多类型探测发现特定接入类型故障。

- **按需调频，按量计费：**
频率最快可达秒级探测；根据业务敏感度灵活调配探测机制和频率。
- **广域网故障链路可视：**
广域网逐跳路径展示，快速诊断异常断点。

如何使用广域网质量监控

初次体验广域网质量监控？别担心，仅需简单几步。先登录[云监控服务 CES](#)，选定“网络性能监控 > 广域网质量监控”即可开通。计费按实际使用量计算，清晰透明。快来试试吧！

说明

- 开通广域网质量监控不会产生任何费用，当用户使用广域网质量监控功能时，将按照实际使用量进行计费。
- 广域网质量监控目前在公测阶段，如需开通，请先点击[提交工单](#)申请公测(每日审批公测名单)。

图 2-3 申请公测

申请公测

申请的公测产品/服务

CES广域网质量监控

申请信息

* 企业规模: 50人以下 | 50-100人 | 100-200人 | 200-500人 | 500人以上

* 研发人员比例: 0%-10%

* 应用场景: web

* 业务当前阶段: 开发 | 测试 | 试运行 | 正式运营

* 业务模式: 华为云员工

* 联系人: 金*

* 联系电话: +355(阿尔巴尼亚) 156****0125

电子邮箱:

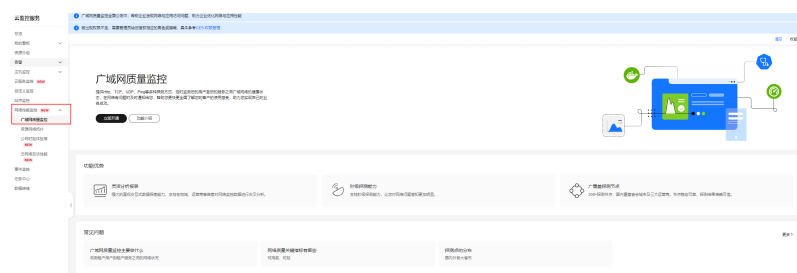
同意《公测试用服务协议》

申请公测

具体操作步骤如下：

1. 登录[云监控服务 CES](#)，点击免费使用，进入CES产品主页。
2. 在左侧导航栏，选择“网络性能监控 > 广域网质量监控”。

图 2-4 广域网质量监控



3. 在首次使用广域网质量监控前，需要单独开通。单击“立即开通”，详情参见：[开通广域网质量监控](#)。
4. 在“开通广域网质量监控”页面，可查看计费模式和计费说明。单击“立即开通”，即可开通。在“开通成功”页面，单击“确定”。

计费标准

广域网质量监控支持以下两种计费方式：

- 按需计费

计费方式	探测点类型	探测点位置	单价（元/次）
按需计费	PC端	中国	0.001
	PC端	海外	0.005

- 包月资源包计费：请参见[购买广域网质量监控资源包](#)。

计费方式	规格（次/月）	总价（元/月）	单价（元/万次）
资源包计费	3000	0	0
	1万	8	8
	5万	40	8
	20万	160	8
	50万	400	8
	100万	750	7.5
	150万	1125	7.5
	200万	1400	7

结束语

总之，网络与服务的稳定性占据着举足轻重的地位，拨测技术作为保障网络和服务稳定性的有力武器，助力企业实现主动式监控，全方位洞察服务的可用性、性能瓶颈等问题。通过合理选择分布的探测节点，制定多层次的拨测策略，企业得以构建起一套严密的监测防护网，能够精准捕捉潜在故障。同时，依据拨测数据的深度分析，企业还能对资源配置进行精细化调整，消除冗余，提升效能，实现业务流程的高效流转。最终，为企业呈上更加稳定可靠、流畅便捷的服务。

产品入口

欢迎大家来体验来自华为云云监控的拨测产品，产品入口：[云监控服务 CES](#)

3 服务优势

自动开通

云监控服务会自动开通。同时您可以很方便使用云监控服务管理控制台或API接口查看云服务运行状态并设置告警规则。

实时可靠

原始采样数据实时上报，提供对云服务的实时监控，实时触发产生告警并通知用户。

监控可视化

云监控服务通过监控面板为用户提供丰富的图表展现形式，支持数据自动刷新以及指标对比查看，满足用户多场景下的监控数据可视化需求。

多种通知方式

通过在告警规则中开启消息通知，当云服务的状态变化触发告警规则设置的阈值时，系统提供电话、短信、邮箱、企业微信、钉钉、飞书和WeLink通知，还可以通过HTTP、HTTPS将告警信息发送至告警服务器，用户可以在第一时间知悉业务运行状况，便于构建智能化的程序处理告警。

批量创建告警规则

告警模板可以帮助用户为多个云服务快速创建告警规则，极大的提高了维护人员的工作效率。

4 应用场景

云监控服务为用户提供了非常丰富的使用场景。

云服务监控

用户开通了云监控服务支持的云服务后，即可方便地在云监控Console页面查看您的云产品运行状态和相关指标数据，并对监控项创建告警规则。

主机监控

通过监控ECS或BMS的CPU使用率、内存使用率、磁盘等基础指标，确保ECS或BMS的正常使用，避免因对资源的过度使用造成业务无法正常运行。

处理异常场景

云监控服务会根据您创建的告警规则，在监控数据达到告警策略时发送告警信息，让您及时获取异常通知，查询异常原因。

扩容场景

对CPU使用率、内存使用率、磁盘使用率等监控项创建告警规则后，可以让您方便的了解云服务现状，在业务量变大后及时收到告警通知进行手动扩容，或配合弹性伸缩服务自动伸缩。

站点监控

站点监控服务目前提供HTTP(HTTPS)、TCP、UDP、PING 4种探测协议，可探测您站点的可用性、响应时间、丢包率等，让您全面了解站点的可用性并在异常时及时处理。

自定义监控

自定义监控补充了云服务监控的不足，当云监控服务未能提供您需要的监控项，那么您可以创建自定义监控项并采集监控数据上报到云监控服务，云监控服务会对自定义监控项提供监控图表展示和告警功能。

日志监控

日志监控提供了针对日志内容的实时监控能力。通过云监控服务和云日志服务的结合，用户可以针对日志内容进行监控统计、设置告警规则等，降低用户监控日志的运维成本，简化用户使用监控日志的流程。

事件监控

事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。

5 服务资费

云监控服务基础功能免费，包括查看监控看板、创建告警规则、添加监控项等。同时云监控服务与其他云服务组合使用，为您提供监控数据文件转储、发送告警通知等增值服务，这些增值服务可能产生额外费用，具体由提供该功能的服务结算。

通常情况下，云监控服务产生的增值服务费用很低，因此建议您根据需要搭配使用。

增值服务列表如下：

- **监控数据文件转储：**需要使用对象存储服务（OBS），转储后的监控数据文件将永久保存。
- **发送告警通知：**需要使用消息通知服务（SMN），当云服务的状态变化触发告警规则设置的阈值时，发送邮件、短信、HTTP、HTTPS告知用户。

增值服务的计费方式如下：

- **对象存储服务（OBS）**

对象存储服务提供按需付费、包年包月两种计费方式。用户可以根据实际需求变更资源的资费方式。OBS开通时，默认按照按需付费（转用量按小时计费），同时也支持包年包月（资源包）的方式提前购买使用额度和时长。

由于云监控服务需要高频次的访问转储事件文件的OBS桶，因此必须选择标准存储类型的OBS桶，具体价格请参考[产品价格说明](#)。

- **消息通知服务（SMN）**

消息通知服务会从短信、邮件、HTTP、HTTPS的使用中收费，具体价格请参考[产品价格说明](#)。

6 云监控服务相关概念

使用云监控服务之前，请先了解以下相关概念，从而可以更好的使用云监控服务。

- [监控指标](#)
- [聚合](#)
- [监控面板](#)
- [主题](#)
- [告警规则](#)
- [告警模板](#)
- [项目](#)
- [企业项目](#)

监控指标

监控指标是云监控服务的核心概念，通常是指云平台上某个资源的某个维度状态的量化值，如云服务器的CPU使用率、内存使用率等。监控指标是与时间有关的变量值，会随着时间的变化产生一系列监控数据，帮助用户了解特定时间内该监控指标的变化。

聚合

聚合是云监控服务在特定周期内对各服务上报的原始采样数据采取平均值、最大值、最小值、求和值、方差值计算的过程。这个计算的周期又叫做聚合周期，目前云监控服务支持5分钟、20分钟、1小时、4小时、24小时共五种聚合周期。

监控面板

监控面板为用户提供自定义查看监控数据的功能，支持在一个监控面板跨服务、跨维度查看监控数据，将您关注的重点服务监控指标集中呈现，既能满足总览服务运行概况，又能满足排查故障时快速查看监控详情的需求。

主题

主题是消息通知服务中消息发布或客户端订阅通知的特定事件类型，为用户提供一对多的发布订阅以及消息通知功能，支持用户实现一站式多种消息通知方式。借助消息通知服务，云监控服务在监控到云服务资源发生变化时，通过多种方式通知用户，让用户实时掌握云服务的运行状况。

告警规则

告警规则是指用户对云服务的某个监控指标设置阈值，当告警规则的状态（告警、恢复正常）变化时，支持以邮箱、短信、HTTP、HTTPS等方式通知用户，避免因资源问题造成业务损失。

告警模板

告警模板是一组以服务为单位的告警规则组合，它可以帮助用户快速为多个云服务创建告警规则，极大的提高了维护人员的工作效率。

项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。项目可以是一个部门或者一个项目组。一个账户中可以创建多个项目。

企业项目

企业可以根据组织架构规划企业项目，将企业分布在不同区域的资源按照企业项目进行统一管理，同时可以为每个企业项目设置拥有不同权限的用户组。

云监控服务支持企业项目，只有拥有对应企业项目权限的用户才有权限查看和管理资源分组、告警规则和监控面板。

7 约束与限制

当前云监控服务对单个用户的使用限制如表7-1所示。调整配额请参考[配额调整](#)。

表 7-1 用户资源限制

配额类型	默认限制
可创建告警规则数	1000
可创建自定义告警模板数	200
告警模板可添加告警规则数	50
可创建监控看板数	10
单监控看板可添加监控视图数	50
历史告警保存时间	7天
单次创建告警规则可选择的被监控对象数	5000
单次可创建告警规则条数	1000 说明 若选择监控对象为50个，监控指标为20个，则可创建的告警规则条数为1000。
发送通知可选择主题数	5
单次导出监控数据条数	400 说明 若监控对象为400个，则监控指标为1个。若监控对象为80个，则监控指标为5个。
可创建资源分组个数	1000
单个资源分组单次添加资源数	1000
单个资源分组资源总数	10000
可创建监控站点个数	20
告警模板策略个数	50

8 安全

8.1 责任共担

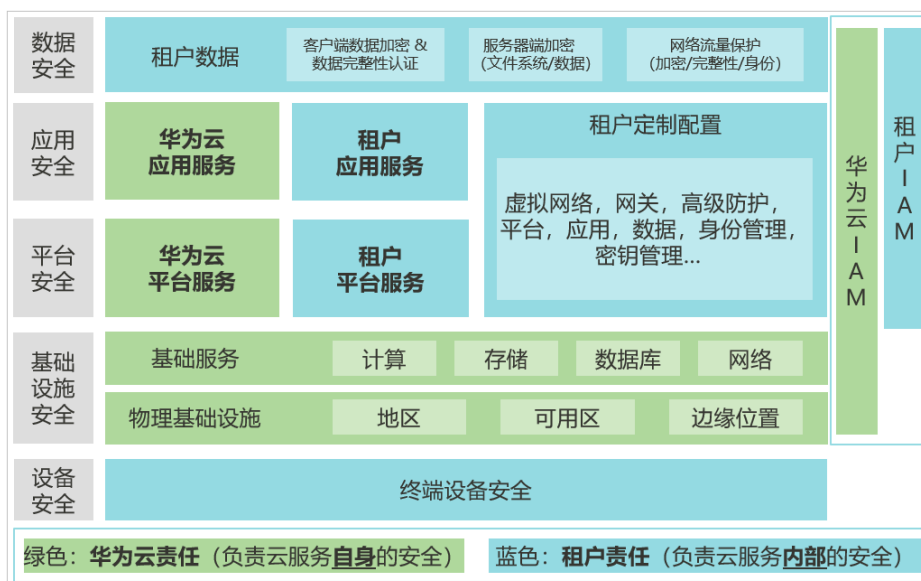
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1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 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

8.2.1 服务的访问控制

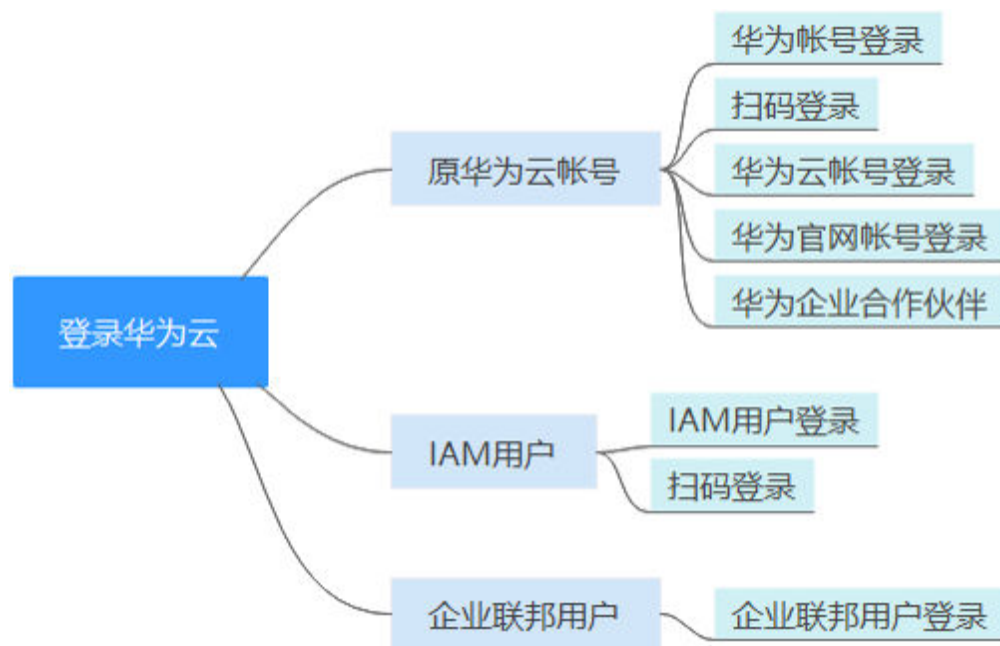
CES对接了华为云**统一身份认证服务（Identity and Access Management, 简称IAM）**。如果您需要对华为云上的CES资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

鉴权

您可以通过以下方式登录华为云，如图8-2所示。

- **华为云账号**：您首次使用华为云时创建的账号，该账号是您的华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限。
- **IAM用户**：由管理员在IAM中创建的用户，是云服务的使用人员，根据账号授予的权限使用资源。
企业联邦用户：由管理员在IAM中创建的企业身份提供商用户。

图 8-2 登录华为云



访问控制

CES基于IAM提供了系统策略和自定义策略，需要给用户配置相应策略，才能创建或访问CES资源，具体操作步骤参考：[创建用户并授权使用云监控服务](#)。建议您使用自定义策略，定义CES所需的最小权限集合即可。

8.3 审计与日志

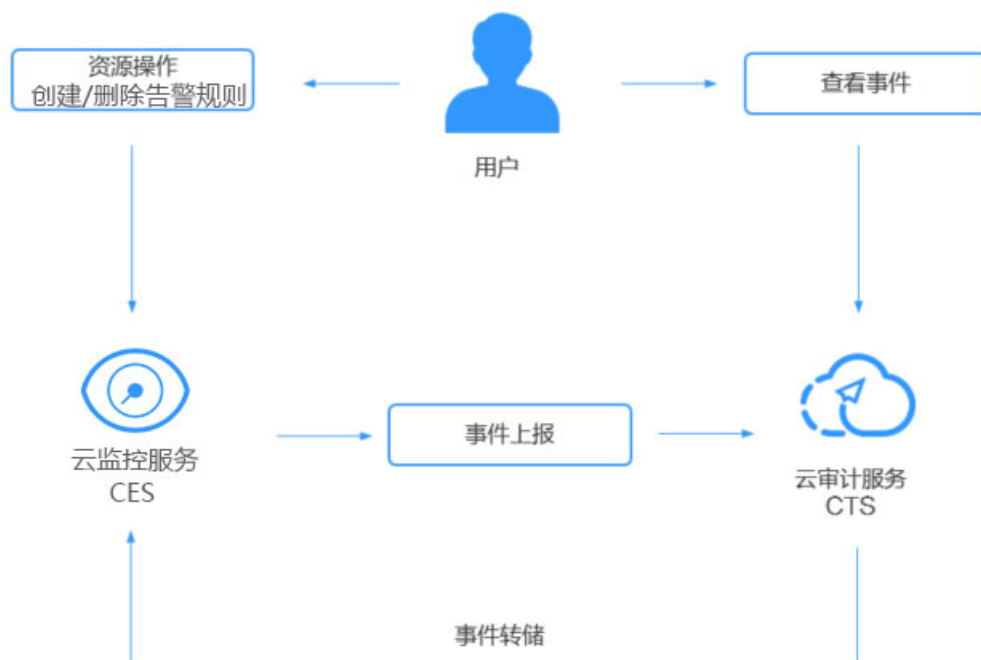
审计

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。

用户开通云审计服务并创建和配置追踪器后，CTS可记录CES的管理事件和数据事件用于审计。

- CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。
- CES支持审计的操作事件请参见[云审计服务支持的Cloud Eye操作列表](#)。

图 8-3 云审计服务



日志

在您开启了云审计服务后，系统开始记录云监控资源的操作。云审计服务管理控制台保存最近7天的操作记录。如何在云审计服务管理控制台查看或导出最近7天的操作记录，请参见[查看云监控服务日志](#)。

8.4 数据保护技术

出于数据保护目的，我们建议您保护华为云帐户凭据，并使用华为云统一身份认证服务（IAM）设置单个用户帐户。这样每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据安全：

- 对每个帐户使用多因素身份验证（MFA）。
- 使用SSL/TLS与华为云资源通信。我们建议使用TLS 1.2或更高版本。
- 使用Cloud Trace Service设置API和用户活动日志记录。
- 使用Data Encryption Workshop，以及华为云服务中的所有默认安全控制。

我们强烈建议您切勿将机密或敏感信息（如客户的电子邮件地址）放入标记或自由表单域中，如名称字段。这包括使用控制台、API、华为云CLI或华为云SDK使用CES或其他华为云服务时。您输入到标记或用于名称的自由表单域中的任何数据都可用于计费或诊断日志。如果您提供了外部服务器的URL，我们强烈建议您不要在URL中包括凭据信息，以验证您对该服务器的请求。

传输中的加密

CES对传输中的数据使用端到端加密。

9 区域和可用区

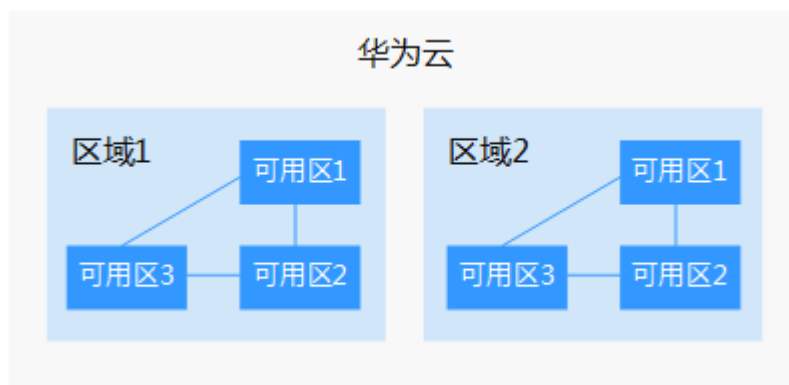
什么是区域、可用区？

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图9-1阐明了区域和可用区之间的关系。

图 9-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见[华为云全球站点](#)。

如何选择区域？

选择区域时，您需要考虑以下几个因素：

- 地理位置

一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

- 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
- 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
- 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

 说明

“拉美-圣地亚哥”区域位于智利。

- 资源的价格

不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

10 权限管理

如果您需要对华为云上的云监控服务资源，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，您希望他们拥有云监控服务的使用权限，但是不希望他们拥有删除其他云服务资源等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用云监控服务，但是不允许删除其他云服务资源的权限策略，控制他们对其他云服务资源的使用范围。

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，不影响您使用云监控服务的其它功能。

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。关于IAM的详细介绍，请参见[什么是IAM](#)。

云监控服务权限

默认情况下，新建的IAM用户没有任何权限，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。

Cloud Eye部署时通过物理区域划分，为项目级服务，需要在各区域（如华北-北京1）对应的项目（cn-north-1）中设置策略，并且该策略仅对此项目生效，如果需要所有区域都生效，则需要所有项目都设置策略。访问Cloud Eye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。

- **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：针对云监控服务，管理员能够控制IAM用户仅能对某一类云监控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，权限的最小粒度为API授权项（action），云监控服务支持的API授权项请参见[策略及授权项说明](#)。

如表10-1所示，包括了云监控服务的所有系统权限。

表 10-1 云监控服务系统权限

系统角色/策略名称	描述	类别	依赖关系
CES FullAccessPolicy	云监控服务的全部权限，拥有该权限可以操作云监控服务的全部权限。	系统策略	云服务监控功能涉及需要查询其他云服务的实例资源，该策略中已包含部分云服务的资源查询权限，如在使用中遇到权限问题，需要配置涉及服务的细粒度授权特性，才可以正常使用，支持细粒度授权的云服务列表请参考： 使用IAM授权的云服务 。 告警通知：依赖SMN服务的SMN FullAccess。 配置数据转储：依赖OBS服务的OBS OperateAccess。
CES ReadOnlyAccessPolicy	云监控服务的只读权限，拥有该权限仅能查看云监控服务的数据。	系统策略	云服务监控功能涉及需要查询其他云服务的实例资源，该策略中已包含部分云服务的资源查询权限，如在使用中遇到权限问题，需要配置涉及服务的细粒度授权特性，才可以正常使用，支持细粒度授权的云服务列表请参考： 使用IAM授权的云服务 。
CES AgentAccess	CES Agent正常运行所需的必要权限。 说明 为了保证CES Agent能够正常提供服务，需要配置委托，详细操作请参见 如何配置委托?	系统策略	无。
CES SiteMonitor FullAccess	云监控服务站点监控所有权限。	系统策略	无。
CES SiteMonitor ReadOnlyAccess	云监控服务站点监控只读权限。	系统策略	无。
CES Administrator	云监控服务的管理员权限。	系统角色	依赖Tenant Guest策略。 Tenant Guest：全局级策略，在全局项目中勾选。

系统角色/策略名称	描述	类别	依赖关系
CES AgencyCheck Access	云监控服务检查租户委托权限需要授权的IAM操作权限集	系统策略	云服务监控OBS转储、数据转储、主机监控等相关功能所依赖的委托策略集合，该策略中已包含委托需要授权的IAM操作权限集，如在使用OBS转储、数据转储、主机监控等功能时遇到委托相关权限问题，需要配置IAM委托操作的细粒度授权特性，才可以正常使用。
CES Global FullAccess	云监控服务全局业务所有权限	系统策略	云监控服务站点监控、广域网质量监控、告警通知等相关功能所依赖的委托策略集合，该策略中已包含云监控服务的全局业务和云监控服务所依赖的全局服务操作的集合，如在使用站点监控、广域网质量监控、告警通知等功能时遇到权限问题，需要配置该权限集才可以正常使用。
CES FullAccess	云监控服务的全部权限，拥有该权限可以操作云监控服务的全部权限。 说明 CES FullAccess不满足权限最小化原则，后续不推荐使用，建议使用CES FullAccessPolicy	系统策略	云服务监控功能涉及需要查询其他云服务的实例资源，该策略中已包含部分云服务的资源查询权限，如在使用中遇到权限问题，需要配置涉及服务的细粒度授权特性，才可以正常使用，支持细粒度授权的云服务列表请参考： 使用IAM授权的云服务 。 告警通知：依赖SMN服务的SMN FullAccess。 配置数据转储：依赖OBS服务的OBS OperateAccess。
CES ReadOnlyAccess	云监控服务的只读权限，拥有该权限仅能查看云监控服务的数据。 说明 CES ReadOnlyAccess不满足权限最小化原则，后续不推荐使用，建议使用CES ReadOnlyAccessPolicy	系统策略	云服务监控功能涉及需要查询其他云服务的实例资源，该策略中已包含部分云服务的资源查询权限，如在使用中遇到权限问题，需要配置涉及服务的细粒度授权特性，才可以正常使用，支持细粒度授权的云服务列表请参考： 使用IAM授权的云服务 。

表10-2列出了云监控服务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 10-2 常用操作与系统权限的关系

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加 Tenant Guest策略)	Tenant Guest
监控概览	查看监控概览	√	√	√	√	√	√
	查看监控大屏	√	√	√	√	√	√
监控面板	创建监控面板	√	×	√	×	√	×
	查看监控大屏	√	√	√	√	√	√
	查看监控面板	√	√	√	√	√	√
	删除监控面板	√	×	√	×	√	×
	添加监控视图	√	×	√	×	√	×
	查看监控视图	√	√	√	√	√	√
	修改监控视图	√	×	√	×	√	×
	删除监控视图	√	×	√	×	√	×
资源分组	调整监控视图位置	√	×	√	×	√	×
	创建资源分组	√	×	√	×	√	×
	查看资源分组列表	√	√	√	√	√	√
	查看资源分组 (资源概览)	√	√	√	√	√	√
	查看资源分组 (不健康资源)	√	√	√	√	√	√

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加Tenant Guest策略)	Tenant Guest
	查看资源分组 (告警规则)	√	√	√	√	√	√
	查看资源分组 (告警记录)	√	√	√	√	√	√
	修改资源分组	√	×	√	×	√	×
	删除资源分组	√	×	√	×	√	×
告警规则	创建告警规则	√	×	√	×	√	×
	修改告警规则	√	×	√	×	√	×
	启用告警规则	√	×	√	×	√	×
	停用告警规则	√	×	√	×	√	×
	删除告警规则	√	×	√	×	√	×
	导出告警规则	√	×	×	×	√	×
	查看告警规则列表	√	√	√	√	√	√
	查看告警规则详情	√	√	√	√	√	√
	查看监控图表	√	√	√	√	√	√
告警记录	查看告警记录	√	√	√	√	√	√
告警模板	查看默认告警模板	√	√	√	√	√	√

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加Tenant Guest策略)	Tenant Guest
	查看自定义告警模板	√	√	√	√	√	√
	创建自定义告警模板	√	×	√	×	√	×
	修改自定义告警模板	√	×	√	×	√	×
	删除自定义告警模板	√	×	√	×	√	×
一键告警	开启一键告警	√	×	√	×	√	×
	查看一键告警	√	√	√	√	√	√
	修改一键告警	√	×	√	×	√	×
	关闭一键告警	√	×	√	×	√	×
主机监控	查看主机列表	√	√	√	√	√	√
	查看主机监控指标	√	√	√	√	√	√
	安装Agent	√ (需同时拥有ECS FullAccess权限)	×	√	×	√ (需同时拥有ECS FullAccess权限)	×
	修复插件配置	√ (需同时拥有Security Administrator、ECS FullAccess权限)	×	√	×	√ (需同时拥有Security Administrator、ECS FullAccess权限)	×

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加 Tenant Guest策略)	Tenant Guest
	卸载Agent	√ (需同时拥有 ECS FullAccess 权限)	×	√	×	√ (需同时拥有 ECS FullAccess 权限)	×
	配置进程监控	√	×	√	×	√	×
	配置自定义进程监控	√	×	√	×	√	×
云服务监控	查看云服务列表	√ (涉及云服务需要支持细粒度授权特性, 参考: 使用IAM授权的云服务)	√ (涉及云服务需要支持细粒度授权特性, 参考: 使用IAM授权的云服务)	√	√	√	√
	查看云服务监控指标	√	√	√	√	√	√
站点监控	创建站点监控	√ (站点监控部署在华北-北京一, 若在其他 Region 使用站点监控功能, 需同时添加华北-北京一的权限)	×	√	×	√ (站点监控部署在华北-北京一, 若在其他 Region 使用站点监控功能, 需同时添加华北-北京一的权限)	×
	查看站点监控列表	√	√	√	√	√	√

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加Tenant Guest策略)	Tenant Guest
	查看站点监控详情	√	√	√	√	√	√
	修改站点监控	√	×	√	×	√	×
	启用站点监控	√	×	√	×	√	×
	停用站点监控	√	×	√	×	√	×
	删除站点监控	√	×	√	×	√	×
自定义监控	添加自定义监控数据	√	×	√	√	√	×
	查看自定义监控列表	√	√	√	√	√	√
	查看自定义监控数据	√	√	√	√	√	√
事件监控	添加自定义事件	√	×	√	√	√	×
	查看事件列表	√	√	√	√	√	√
	查看事件详情	√	√	√	√	√	√
日志监控	自定义指标过滤配置	√ (需同时拥有LTS FullAccess权限)	×	√	×	√ (需同时拥有LTS FullAccess权限)	×
	查看日志监控列表	√	√	√	√	√	√
	查看日志监控详情	√	√	√	√	√	√

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Site Monitor Full Access	CES SiteMonitorReadOnlyAccess	CES Administrator (需同时添加Tenant Guest策略)	Tenant Guest
数据转储到DMS Kafka	创建数据转储任务	√	×	√	×	√	×
	查询数据转储任务列表	√	√	√	√	√	√
	查询指定数据转储任务	√	√	√	√	√	√
	修改数据转储任务	√	×	√	×	√	×
	启动数据转储任务	√	×	√	×	√	×
	停止数据转储任务	√	×	√	×	√	×
	删除数据转储任务	√	×	√	×	√	×
其他	配置数据转储	√ (需同时拥有OBS Bucket Viewer权限)	×	√	×	√ (需同时拥有Tenant Administrator权限)	×
	导出监控数据	√	×	×	×	√	×
	发送告警通知	√	×	√	×	√	×

云监控控制台功能依赖的角色或策略

如果IAM用户需要在云监控服务控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了CES Administrator、CES FullAccess或CES ReadOnlyAccess策略的集群权限，再按如下表10-3增加依赖服务的角色或策略。

表 10-3 云监控控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
云服务监控	<ul style="list-style-type: none">● 云手机服务器 CPH● ROMA Connect:<ul style="list-style-type: none">- 业务流 BFS- 快速数据集成 FDI- 服务集成 APIC● 云搜索服务 CSS● 云桌面 Workspace● 消息&短信服务 MSGSMS	支持设置了CES Administrator、CES FullAccess或CES ReadOnlyAccess权限的IAM用户查看云服务监控信息。

相关链接

- [IAM产品介绍](#)
- 创建用户组、用户并授予CES权限请参考：[创建用户并授权使用云监控服务](#)
- 细粒度策略支持的授权项，请参见《云监控服务API参考》中的[策略和授权项说明](#)。