云监控服务

产品介绍

文档版本 01

发布日期 2025-10-27

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 什么是云监控服务?

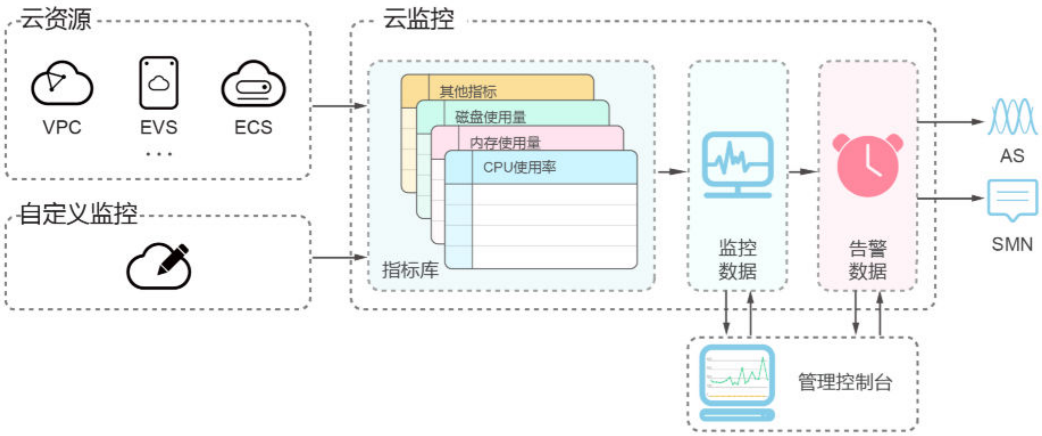
云监控服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

产品架构

云监控服务作为一个监控平台，接收来自各类云服务上报的监控指标，同时也支持用户通过API接口，根据云监控服务规定的上报规范，自定义上报监控指标。

所有的监控指标存储在云监控服务的后台指标库中，当云服务资源有监控数据上报给云监控服务时，对应的云服务的监控指标会呈现在云监控服务的默认指标视图中，用户可以直观地在视图上查看资源的各种监控数据，还可以基于监控指标在业务上的重要程度配置不同级别的告警规则，当监控指标数据达到告警阈值后即可触发告警，并通过SMN消息通知服务的各种通知渠道将告警发送给用户。用户收到告警后可以及时对资源异常做出响应。

图 1-1 云监控服务架构图



主要功能

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。有关告警规则的更多信息，请参阅**告警规则简介**。

- 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、HTTP、HTTPS、FunctionGraph（函数）、FunctionGraph（工作流）、企业微信、钉钉、飞书或Welink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。有关告警通知的更多信息，请参阅**告警通知**。

- 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。有关监控面板的更多信息，请参阅**我的看板简介**。

- 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。有关资源分组的更多信息，请参阅**资源分组简介**。

- 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。有关事件监控的更多信息，请参阅**事件监控简介**。

- 数据转储：

  当您需要通过分布式消息服务Kafka的控制台或使用开源Kafka客户端查询云服务的监控指标时，可以使用云监控服务提供的数据转储功能。数据转储可以实时将云服务监控数据转储到分布式消息服务Kafka中。

2 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，系统提供短信、邮件、FunctionGraph（函数）、FunctionGraph（工作流）、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，极大地提高了维护人员的工作效率。

3 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，避免因为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，可以让您方便地了解云服务现状，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。

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。

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。

4 产品功能

本页面介绍了云监控服务支持的主要功能。关于各功能支持的地域（Region）信息，可通过控制台查询详情。

监控看板

监控看板为您提供自定义查看监控数据的功能，将您关注的核心服务监控指标集中呈现在一张监控面板里，为您定制一个立体化的监控平台。同时监控面板还支持在一个监控项内对不同服务、不同维度的数据进行对比查看，帮助您实现不同云服务间性能数据对比查看的需求。

在添加监控视图之前，需要先创建监控面板。目前云监控服务默认支持创建10个监控面板，满足您对云服务运行情况不同的监控需求。有关看板的更多信息，请参见**创建自定义监控看板**。

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、告警历史，可以迅速提升运维效率。

资源分组支持企业项目，当选择了资源分组到某个企业项目时，只有拥有该企业项目权限的用户才可以查看和管理该资源分组。

有关资源分组的更多信息，请参见**创建资源分组**。

主机监控

主机监控分为基础监控、操作系统监控和进程监控。无论您使用的是弹性云服务器还是裸金属服务器，都可以使用主机监控来采集丰富的操作系统层面监控指标，也可以使用主机监控进行服务器资源使用情况监控和排查故障时的监控数据查询。

- **基础监控**：ECS自动上报的监控指标，数据采集频率为5分钟1次。可以监控CPU使用率等指标，详见**云产品监控指标**。
- **操作系统监控**：通过在弹性云服务器或裸金属服务器中安装Agent插件，为用户提供服务器的系统级、主动式、细颗粒度监控服务。数据采集频率为1分钟1次。除了CPU使用率等指标外，还可以支持内存使用率（Linux）等指标，详见**云产品监控指标**。
- **进程监控**：针对主机内活跃进程进行的监控，默认采集活跃进程消耗的CPU、内存，以及打开的文件数量等信息。

有关主机监控的更多信息，请参见**概览**。

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。事件即云监控服务保存并监控的云服务资源的关键操作，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，如删除虚拟机、重启虚拟机等。

事件监控默认开通，您可以在事件监控中查看系统事件和自定义事件的监控详情，目前支持的系统事件请参见**事件监控支持的事件说明**。

有关事件监控的更多信息，请参见**查看事件监控数据**。

告警功能

告警功能提供对监控指标的告警功能，用户对云服务的核心监控指标设置告警规则，当监控指标触发用户设置的告警条件时，支持以邮箱、短信、HTTP、HTTPS等方式通知用户，让用户在第一时间得知云服务发生异常，迅速处理故障，避免因资源问题造成业务损失。

云监控服务使用消息通知服务向用户通知告警信息。首先，您需要在消息通知服务界面创建一个主题并为这个主题添加相关的订阅者，然后在添加告警规则的时候，您需要开启消息通知服务并选择创建的主题，这样在云服务发生异常时，云监控服务可以实时的将告警信息以广播的方式通知这些订阅者。

告警规则支持企业项目，当选择了告警规则到某个企业项目时，只有拥有该企业项目权限的用户才可以查看和管理该告警规则。

有关告警功能的更多介绍，请参见**告警简介**。

权限管理

如果您需要对您所拥有的云监控服务进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用云监控服务。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将云监控服务的相关操作委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

有关权限管理的更多介绍，请参见**创建用户并授权使用云监控服务**

APIs

云监控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。

您可以使用API对指标、告警规则、监控数据进行相关操作，如查询指标列表、查询告警规则列表、创建告警规则、删除告警规则等。支持的全部操作请参见**API概览**。

在调用云监控服务API之前，请确保已经充分了解云监控服务相关概念，详细信息请参见**产品介绍**。

5 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，从而可以更好地使用云监控服务。

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。如何查看云服务监控数据，请参阅**查看云服务监控看板**。云监控服务支持的监控指标，请参阅**云产品监控指标**。

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。有关聚合的更多信息，请参阅**什么是聚合**。

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。有关监控面板的更多信息，请参阅**我的看板简介**。

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。有关主题的更多信息，请参阅**创建主题**。

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，支持以邮件、短信、HTTP、HTTPS、FunctionGraph（函数）、FunctionGraph（工作流）、企业微信、钉钉、飞书和Welink等方式通知用户，避免因资源问题造成业务损失。有关告警规则的更多信息，请参阅**创建告警规则和通知**。

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，极大地提高了维护人员的工作效率。有关告警模板的更多信息，请参阅**创建自定义告警/事件模板**。

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。有关项目的更新信息，请参阅**项目**。

维度

资源可以按不同的维度进行分类，例如弹性云服务资源可以分为云服务器、云服务器-磁盘、云服务器-挂载点等多个维度。通过维度可以帮助用户从不同角度对监控指标进行分析，从而更精准地定位问题。

根据使用场景的不同，维度会由单个或多个层级组成，在使用API接口查询多层级维度的监控数据时，需要结合维度的层级关系进行查询。

6 约束与限制

当前云监控服务对单个用户的默认使用限制如表6-1所示。调整配额请参考配额调整。

表 6-1 用户资源限制

配额类型	默认限制
可创建告警规则数	1000
可创建告警模板数	200
告警模板中单个服务可添加的告警策略数	50
可创建监控看板数	10
单监控看板可添加监控视图数	50
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	20
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。

7 安全

7.1 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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图7-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 7-1 华为云安全责任共担模型

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图7-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

7.2 身份认证与访问控制

7.2.1 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，可以帮助您安全地控制华为云资源的访问。

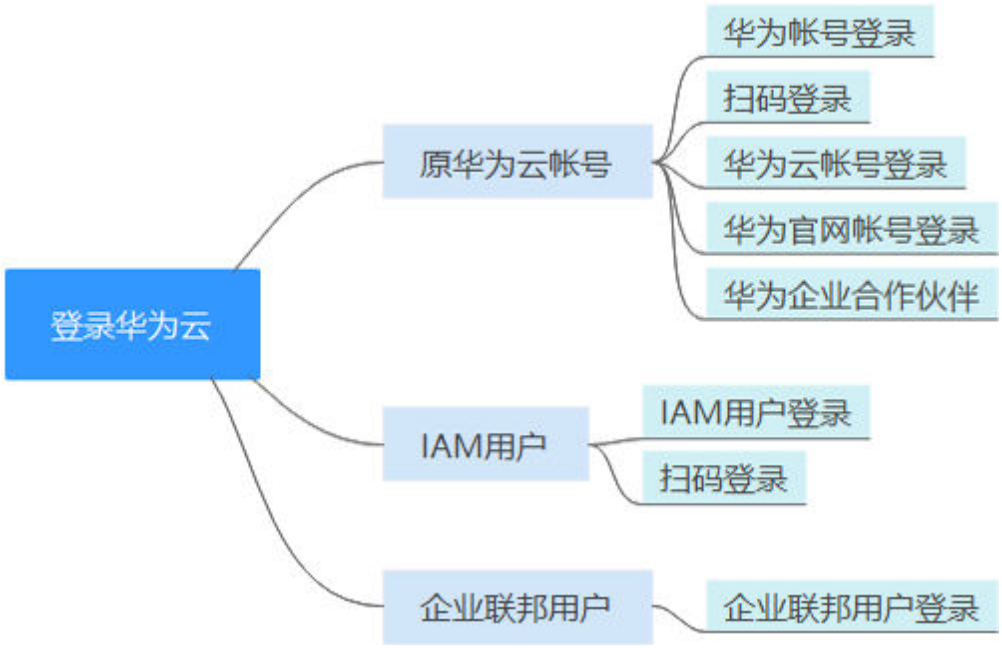
鉴权

您可以通过以下方式登录华为云，如图7-2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 7-2 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：**通过IAM角色或策略授予使用云监控服务的权限**。建议您使用自定义策略，定义CES所需的最小权限集合即可。

7.3 审计与日志

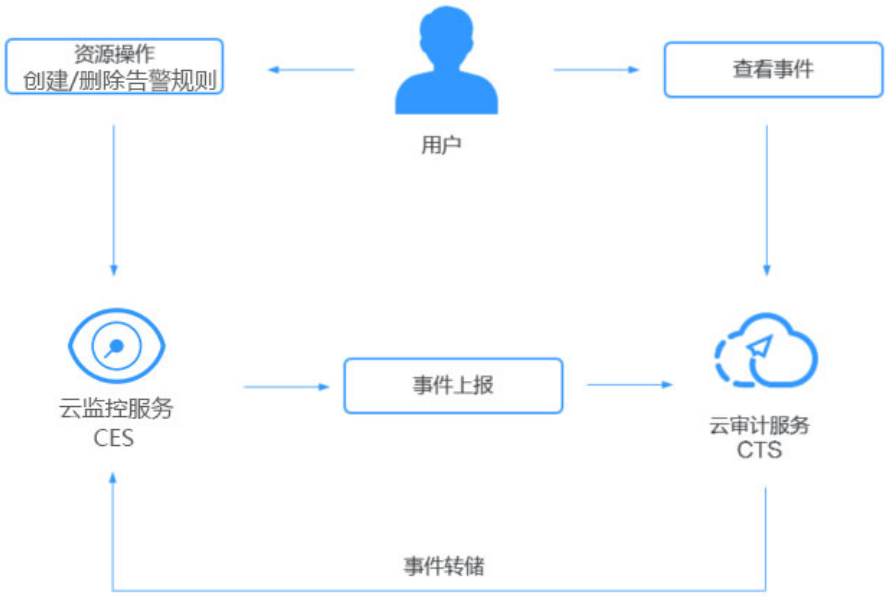
审计

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 7-3 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**。

7.4 数据保护技术

出于数据保护目的，我们建议您保护华为云账号凭据，并使用华为云统一身份认证服务（IAM）设置单个用户账号。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：

- 对每个账号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。

8 区域和可用区

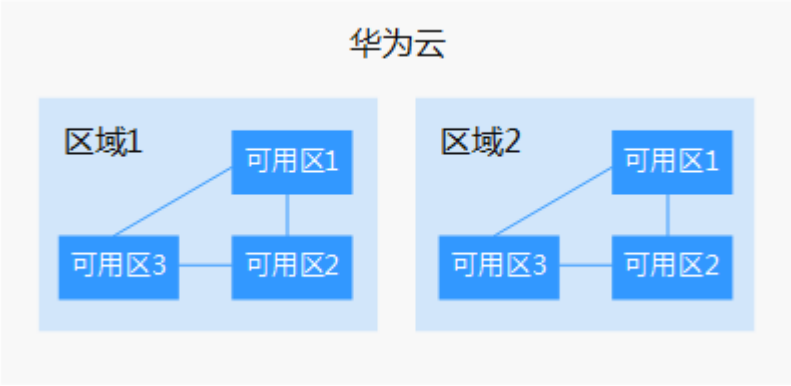
什么是区域、可用区?

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8-1阐明了区域和可用区之间的关系。

图 8-1 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**。

9 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，可以帮助您安全地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（如中国-香港）对应的项目（ap-southeast-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，则需要在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9-1**所示，包括了云监控服务的所有系统权限。

表 9-1 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 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 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9-2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 9-2 常用操作与系统权限的关系

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	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	√	√	√	√
监控大盘	创建监控大盘	√	×	√	×
	查看监控大盘	√	√	√	√
	查看监控大屏	√	√	√	√
	添加监控视图	√	×	√	×
	查看监控视图	√	√	√	√

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator（需同时添加Tenant Guest策略）	Tenant Guest
	修改监控视图	√	×	√	×
	删除监控视图	√	×	√	×
	调整监控视图位置	√	×	√	×
	删除监控大盘	√	×	√	×
我的看板	创建我的看板	√	×	√	×
	查看监控大屏	√	√	√	√
	查看我的看板	√	√	√	√
	删除我的看板	√	×	√	×
	添加监控视图	√	×	√	×
	查看监控视图	√	√	√	√
	修改监控视图	√	×	√	×
	删除监控视图	√	×	√	×
	调整监控视图位置	√	×	√	×
资源分组	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（告警规则）	√	√	√	√
	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	√	×	√	×

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator（需同时添加Tenant Guest策略）	Tenant Guest
	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	√	√	√	√
	查看监控详情	√	√	√	√
	屏蔽告警	√	×	√	×
	手动恢复告警记录	√	×	√	×
告警模板	查看默认告警模板	√	√	√	√
	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）	×

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator（需同时添加Tenant Guest策略）	Tenant Guest
	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）	×
	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	√	√	√	√
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	√	√	√	√
数据转储到DMS Kafka	创建数据转储任务	√	×	√	×

功能	操作	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator（需同时添加Tenant Guest策略）	Tenant Guest
	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 FullAccessPolicy或CES ReadOnlyAccessPolicy策略的集群权限，再按如下**表9-3**增加依赖服务的角色或策略。

表 9-3 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	• 云手机服务器 CPH • ROMA Connect： – 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 FullAccessPolicy或CES ReadOnlyAccessPolicy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，请参考《云监控服务API参考》中“**策略和授权项说明**”章节。