00 产品介绍

文档版本 01

发布日期 2025-02-28

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

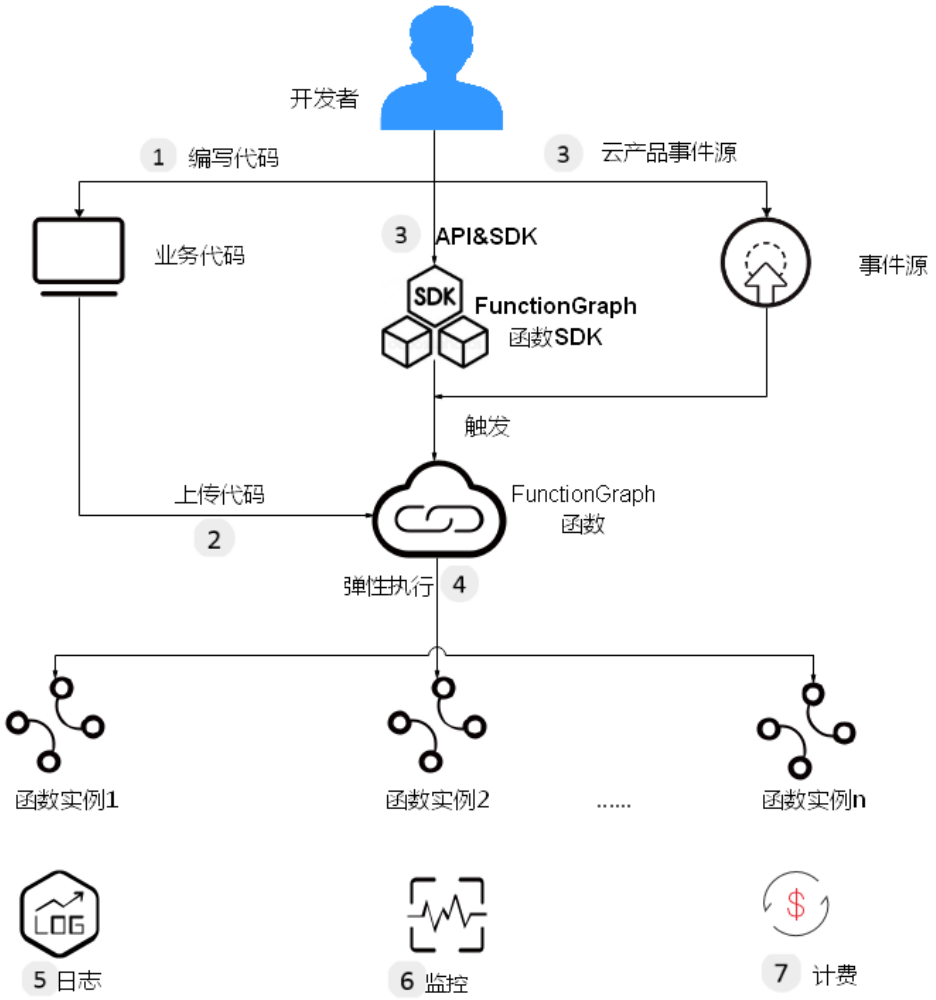
1 图解函数工作流服务

2 什么是 FunctionGraph

FunctionGraph是一项基于事件驱动的函数托管计算服务。使用FunctionGraph函数，只需编写业务函数代码并设置运行的条件，无需配置和管理服务器等基础设施，函数以弹性、免运维、高可靠的方式运行。此外，按函数实际执行资源计费，不执行不产生费用。

函数使用流程如图2-1所示。

图 2-1 函数使用流程



功能简介

①编写代码

用户编写业务代码，目前支持Node.js、Python、Java、Go、C#、PHP、Cangjie等语言，详情请参考**开发指南**。

②上传代码

目前支持在线编辑、上传ZIP或JAR包，从OBS引用ZIP包等，详情请参考**代码上传方式说明**。

③API和云产品事件源触发函数执行

通过RESTful API或者云产品事件源触发函数执行，生成函数实例，实现业务功能。

④弹性执行

函数在执行过程中，会根据请求量弹性扩容，支持请求峰值的执行，此过程用户无需配置，由FunctionGraph完成，并发数限制请参考**约束与限制**。

⑤查看日志

FunctionGraph函数实现了与云日志服务的对接，您无需配置，即可查看函数运行日志信息，请参考**查询日志**。

⑥查看监控

FunctionGraph函数实现了与应用运维管理服务的对接，您无需配置，即可查看图形化监控信息。

⑦计费方式

函数执行结束后，根据函数请求执行次数和执行时间计费。

3 产品功能

函数管理

提供控制台管理函数。

- 函数支持Node.js、Java、Python、Go、PHP、Cangjie等多种运行时语言，同时支持用户自定义运行时，说明如表3-1所示。

  说明

  建议使用相关语言的最新版本。

  表 3-1 运行时语言说明

运行时语言	支持版本
Node.js	6.10、8.10、10.16、12.13、14.18、16.17、18.15
Python	2.7、3.6、3.9、3.10
Java	8.0、11
Go	1.x
C#	.NET Core 2.1、.NET Core 3.1
PHP	7.3
定制运行时	-
Cangjie	1.0

- 函数支持多种代码导入方式

  支持在线编辑代码、OBS文件引入、上传ZIP包、上传JAR包等方式。不同运行时支持的代码上传方式如表3-2所示。

表 3-2 代码上传方式说明

运行时	在线编辑	上传ZIP文件	上传JAR包	从OBS上传文件
Node.js	支持	支持	不支持	支持
Python	支持	支持	不支持	支持
Java	不支持	支持	支持	支持
Go	不支持	支持	不支持	支持
C#	不支持	支持	不支持	支持
PHP	支持	支持	不支持	支持
定制运行时	支持	支持	不支持	支持
Cangjie	不支持	支持	不支持	支持

触发器

函数多种类型触发器，触发器调用方式如表3-3所示。

表 3-3 函数触发方式说明

触发器	函数调用方式
SMN触发器	异步调用
APIG触发器	同步调用
DIS触发器	异步调用
TIMER触发器	异步调用
LTS触发器	异步调用
CTS触发器	异步调用
DDS触发器	异步调用
Kafka触发器	异步调用
分布式消息服务 Kafka版	同步调用

日志和监控

提供调用函数的监控指标和运行日志的采集和展示，实时的图形化监控指标展示，在线查询日志，方便用户查看函数运行状态和定位问题。

日志的查询过程请参考**管理函数日志**。

单个监控指标请参考**监控信息说明**。

租户函数监控指标请参考**总览页面介绍**。

初始化功能

引入initializer接口：

- 分离初始化逻辑和请求处理逻辑，程序逻辑更清晰，让用户更易写出结构良好，性能更优的代码。
- 用户函数代码更新时，系统能够保证用户函数的平滑升级，规避应用层初始化冷启动带来的性能损耗。新的函数实例启动后能够自动执行用户的初始化逻辑，在初始化完成后再处理请求。
- 在应用负载上升，需要增加更多函数实例时，系统能够识别函数应用层初始化的开销，更准确的计算资源伸缩的时机和所需的资源量，让请求延时更加平稳。

函数流

函数流是用来编排FunctionGraph函数的工具，可以将多个函数编排成一个协调多个分布式函数任务执行的工作流。

用户通过在可视化的编排页面，将事件触发器、函数和流程控制器通过连线关联在一个流程图中，每个节点的输出作为连线下一个节点的输入。编排好的流程会按照流程图中设定好的顺序依次执行，执行成功后支持查看工作流的运行记录，方便您轻松地诊断和调试。

函数流功能特性和优势：

- 功能特性
  a. 函数可视化编排
  b. 函数流执行引擎
  c. 错误处理
  d. 可视化监控
- 优势
  a. 使用更少代码快速构建应用程序

     函数流允许用户将函数组合编排成一个完整的应用程序，而无需进行代码编写。可以实现快速构建，快速上线。当业务调整时，可以快速调整流程，完成快速上线，无需编写任何代码。
  b. 完善的错误处理机制

     支持对流程中发生的错误进行捕获和重试，用户可以进行灵活的异常处理。
  c. 可视化的编排和监控体验

     通过拖拽进行流程编排，学习成本低，可以快速上手。

     监控页面使用流程可视化的查看方式，可以做到快速识别问题位置。

统一插件开发和调试

- **VSCode插件支持**（云下）：

  通过模板创建函数，在云端查看函数并下载到本地调试，使用VSCode插件调试，将本地函数推送到云端。

HTTP 函数

该特性仅FunctionGraph v2版本支持。

HTTP函数专注于优化 Web 服务场景，用户可以直接发送 HTTP 请求到 URL 触发函数执行。在函数创建编辑界面增加类型。HTTP函数只允许创建APIG/APIC的触发器类型，其他触发器不支持。

调用链

用户通过页面函数配置开启调用链，开启后可以链接到APM服务页面查看jvm、调用链等信息，当前仅支持JAVA函数。

自定义镜像

该特性仅FunctionGraph v2版本支持。

支持用户直接打包上传容器镜像，由平台加载并启动运行，调用方式与HTTP函数类似。与原来上传代码方式相比，用户可以使用自定义的代码包，不仅灵活也简化了用户的迁移成本。

4 产品优势

无服务器管理

自动运行用户代码，用户无需配置或管理服务器，专注于业务创新。

高弹性

根据请求的并发数量自动调度资源运行函数，实现透明、准确和实时的伸缩，应付业务峰值的访问。

用户无需关心峰值和空闲时段的资源需要申请多少资源，系统根据请求的数量自动扩容/缩容。自动负载均衡将请求分发到函数运行实例。

同时系统会根据流量负载的模式来智能预热实例，以缓解冷启动对业务的影响。

事件触发

通过事件触发机制，集成多种云服务，满足不同场景需求，获得高效的开发体验。

与云日志服务、云监控服务对接，无需任何配置，即可查询函数日志和监控告警信息，快速排查故障。

高可用

函数运行实例出现异常，系统会启动新的实例处理后续的请求，故障函数实例占用资源将会回收使用。

按量计费

根据代码的调用次数和运行时长计费，代码未运行时不产生费用。

预留实例计费

函数提供预留实例功能，预留实例在创建成功后会执行函数的初始化，并且常驻在执行环境中，彻底消除冷启动对业务的影响。

预留实例根据代码的调用次数、实例存活时长计费。时长计量粒度为60秒。

动态资源指定

函数执行时可根据业务需要动态指定资源规格，最小化资源占用，灵活调度节省成本。

5 应用场景

函数工作流应用场景，如实时文件处理、实时数据流处理、Web移动应用后端和人工智能场景。

场景一：事件驱动类应用

以事件驱动的方式执行服务，按需供给，开发者无需关注业务波峰波谷，节省闲时成本，最终降低运维成本。比如视频直播/转码、实时数据流处理、IoT规则/事件处理等。

- **实时文件处理**

  客户端上传文件到OBS，触发FunctionGraph函数，在上传数据后立即进行处理。可以使用FunctionGraph实时创建图像缩略图、转换视频编码、进行数据文件汇聚、筛选等。

  其优势有：

  - 灵活扩展，业务爆发时可以自动调度资源运行更多函数实例以满足处理需求。
  - 事件触发，通过上传文件到OBS，触发FunctionGraph函数进行文件处理。
  - 按需收费，只有对函数处理文件数据的时间进行计费，无需购买冗余的资源用于非峰值处理。

- **实时数据流处理**

  使用FunctionGraph和DIS处理实时流数据，跟踪应用程序活动、顺序事务处理、分析数据流、整理数据、生成指标、筛选日志、建立索引、分析社交媒体以及遥测和计量IoT设备数据。

  其优势有：

  - 事件触发，通过DIS流采集数据，批量数据通过事件触发处理函数进行处理。
  - 灵活扩展，业务爆发时可以自动调度资源运行更多函数实例以满足处理需求。
  - 按需收费，只有对函数处理文件数据的时间进行计费，无需购买冗余的资源用于非峰值处理。

场景二：Web 类应用

使用FunctionGraph和其他云服务或租户VM结合，用户可以快速构建高可用，自动伸缩的Web/移动应用后端。比如小程序、网页/App、聊天机器人、BFF等。

其优势有：

- 高可用，利用OBS，Cloud Table的高可用性实现网站数据的高可靠性，利用API Gateway和FunctionGraph的高可用性实现网站逻辑的高可用。
- 灵活扩展，业务爆发时可以自动调度资源运行更多函数实例以满足处理需求。
- 按需收费，只有对函数处理文件数据的时间进行计费，无需购买冗余的资源用于非峰值处理。

场景三：AI 类应用

各行各业智能化深入带来更多的应用开发场景，通常需要集成各类服务快速上线。比如三方服务集成、AI推理、车牌识别。

其优势有：

- 快速搭建，用户上传图像后触发函数工作流执行调用文字识别/内容检测服务针对图像进程处理，并将结果以JSON结构化数据返回。按需使用函数与多个智能服务集成，形成丰富的应用处理场景。并随时根据业务改变对函数处理过程做调整，实现业务灵活变更。
- 简化运维，用户只需开通相关云服务并在函数服务中编写业务逻辑，无需配置或管理服务器，专注于业务创新。业务爆发时可以自动调度资源运行更多函数实例以满足处理需求。
- 按需计费，只有对函数执行的时间及各智能服务处理进行计费，无需购买冗余的资源用于非峰值处理。

6 函数类型

6.1 事件函数

说明

v2版本在创建函数时，页面会出现参数“函数类型”，区分事件函数和HTTP函数。

概述

FunctionGraph支持事件类型函数。事件是指用于触发函数，通常为JSON格式的请求。用户作为事件源（事件的生产者），可以通过云服务平台或CodeArts IDE Online触发函数并进行执行。在函数创建界面可以选择函数类型，事件类型的函数不受触发器类型的限制，当前FunctionGraph支持的所有类型触发器均可用于触发事件函数。

说明

1. FunctionGraph原生支持事件类型函数，在函数创建界面默认选择该类型；
2. 测试函数时在参数配置界面输入用户指定的事件JSON即可完成函数触发；
3. 用户也可以通过FunctionGraph支持的触发器进行事件函数触发；

优势

- 单机编程体验，简单易用

  事件类型函数可以在FunctionGraph函数界面或CodeArts IDE Online界面进行函数编辑或代码包上传，一键式完成函数云上部署，用户无需关心并处理函数的并发、故障恢复等问题。

- 高性能极速运行时

  事件函数提供毫秒级函数启动、函数扩容、函数调用，秒级故障中断检测及秒级故障恢复。

- 便捷完备的工具链

  提供完备的日志、调用链、debug及监控能力，支撑开发者“三步”上线函数应用。

限制

事件函数受限于事件格式（事件源），开发者在开发过程中需要遵循函数平台的函数开发规则。

6.2 HTTP 函数

约束与限制

该特性仅FunctionGraph v2版本支持。

概述

FunctionGraph支持两种函数类型，事件函数和HTTP函数。HTTP函数专注于优化 Web 服务场景，用户可以直接发送 HTTP 请求到 URL 触发函数执行，从而使用自己的Web服务。HTTP函数只允许创建APIG/APIC的触发器类型，其他触发器不支持。

说明

1. HTTP函数支持HTTP/1.1协议。
2. 在函数创建页面，新增一种函数类型“HTTP函数”；
3. HTTP函数执行入口需要设置为**bootstrap**，用户直接写启动命令，**端口统一开放成8000；**

优势

- 丰富的框架支持

  您可以使用常见的 Web 框架（例如 Nodejs Web 框架：Express、Koa）编写 Web 函数，也可以将您本地的 Web 框架服务以极小的改造量快速迁移上云。
- 减少请求处理环节

  函数可以直接接收并处理 HTTP 请求，API 网关不再需要做 json 格式转换，减少请求处理环节，提升 Web 服务性能。
- 编写体验舒适化

  HTTP 函数的编写体验更贴近编写原生 Web 服务，可以使用 Node.js 原生接口，保证和本地开发服务体验一致。

限制

- HTTP函数只允许创建APIG共享版、APIG专享版、APIC的触发器类型，其他触发器不支持。
- 同一个函数支持绑定多个 API 触发器，但所有 API 都必须在一个APIG服务下。
- 针对HTTP函数，用户的HTTP响应体不超过6M。
- 不支持长时运行和异步调用，不支持重试。

7 约束与限制

支持区域

函数工作流服务支持区域详情请参见**地区和终端节点**。

函数配置

表 7-1 函数配置约束与限制

限制项	说明
单个函数下最大允许创建的版本个数	20（含latest版本）
单个函数下最大允许创建的别名个数	10 每个版本仅可以关联到1个别名。
单个函数版本下最大允许创建的触发器总数	10
单个函数下所有环境变量的大小	总长度不能超过4096个字符。
单个账户下最大允许创建的函数个数	400
单个账户下最大允许部署包大小	10GB
单个账户下函数并发执行数	100 如果您的业务有更大的并发执行数需求，请**提交工单**申请。
单个账户下创建预留实例个数	90（单个租户下函数并发执行数*90%） 如果您的业务有更大的预留实例个数需求，请**提交工单**申请。
单个函数下最大允许创建的标签个数	20 使用标签功能前确保已开通TMS服务，未开通TMS服务时无法使用TMS预定义标签能力。

限制项	说明
网络配置	开启“函数访问VPC内资源”时，函数将禁用默认网卡并使用VPC绑定的网卡，是否允许公网访问由配置的VPC决定，开关“函数访问公网”将不生效。
异步配置	当您在配置异步执行通知目标时，不要出现循环调用的情况。
日志配置	• 已关联的默认日志组更改为其他日志组或关闭日志记录时，将无法重新关联默认日志组。 • 单个函数最多可以添加10个标签。

函数代码

表 7-2 函数代码约束与限制

限制项	说明
前端页面上传时，单个代码部署包大小（压缩为.zip/.jar文件）	40MB
调用函数接口时，在线编辑单个函数代码部署包大小（压缩为.zip/.jar文件）	50MB
函数导出资源包大小	50MB以内
调用函数接口时，单个代码部署包原始代码大小	• ZIP格式：解压后原始代码大小为1500M。 • OBS桶：最大可上传300M压缩后的代码包。
前端页面展示代码大小	20MB
私有依赖包	• 直接上传ZIP文件：上传的文件大小限制为10M，如超过10M，请通过OBS上传。 • 从OBS上传文件：格式为OBS URL链接，文件必须为ZIP格式。

函数流

函数流当前仅支持华东-上海一、亚太-新加坡。

表 7-3 函数流约束与限制

限制项	说明
单个账户下最多创建的函数流个数	200 如果您的业务有更大的函数流个数需求，请**提交工单**申请。
单个函数流支持最多节点数	100 如果您的业务有更大的函数流节点数需求，请**提交工单**申请。
标准函数流	标准模式面向普通的业务场景，只支持异步调用。
快速函数流	快速模式面向业务执行时长较短，只支持流程执行时长低于5分钟的场景，不支持执行历史持久化，支持同步和异步调用。

函数运行资源

表 7-4 函数运行资源约束与限制

限制项	说明
临时磁盘空间（“/tmp”空间）	512MB
文件描述符数	2048
进程和线程数（总和）	1024
单个请求最大执行时长	259200秒 若需要调用执行时间超过90秒的函数，请使用异步调用的方式。 如果您的业务有更大的最大执行时长需求，请**提交工单**申请。
函数同步调用请求正文有效负载大小	6MB
函数同步调用响应正文有效负载大小	6MB 返回的字符串或返回体序列化后的JSON字符串默认不大于6MB。具体数据大小会随FunctionGraph系统后台设置产生变化，因为系统后台判断的是序列化之后的数据大小，所以会存在字节级别的误差，误差范围为6MB±100bytes。
函数异步调用请求正文有效负载大小	256KB
单个自定义镜像函数最大允许镜像大小	10GB

限制项	说明
租户级别实例数限制	1000 如果您的业务有更大的实例数需求，请**提交工单**申请。
函数最大申请内存	10G
带宽	无限制
单条日志大小	无限制
Initializer最大运行时间	259200秒 如果您的业务有更大的Initializer最大运行时间需求，请**提交工单**申请。

8 安全

8.1 责任共担

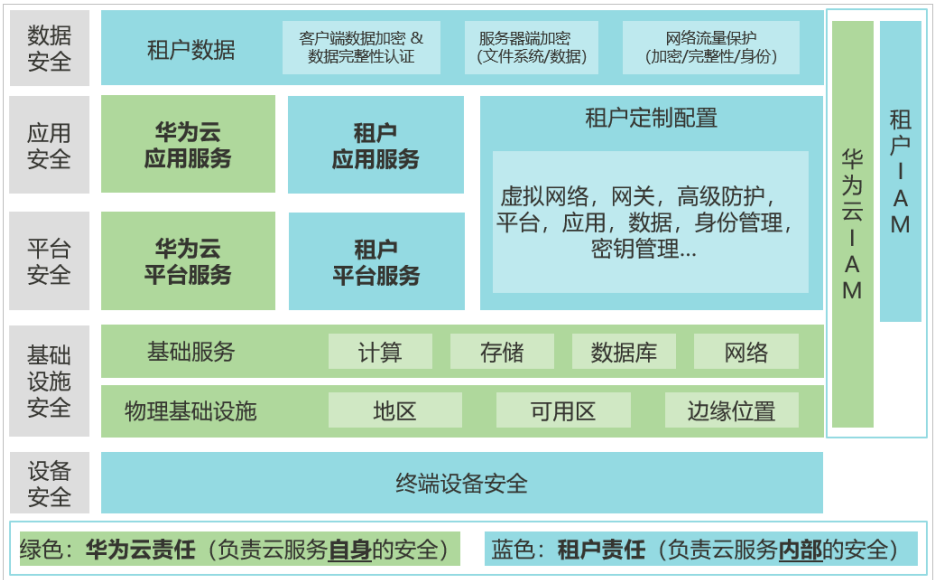
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

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 资产识别与管理

在函数的环境变量中，若有敏感信息例如账号和密码、Ak/Sk等，建议通过配置**加密环境变量**。不配置加密环境变量，则会在界面或API返回结果中明文展示。

在使用触发器、配置VPC访问、使用自定义镜像、挂载SFS等场景下，FunctionGraph需要与其他云服务协同工作，需要由您通过创建云服务委托，让FunctionGraph有权限代替您进行一些资源运维工作。具体请参见**委托配置**。

8.3 身份认证与访问控制

身份认证

用户访问FunctionGraph的方式有多种，包括FunctionGraph控制台、API、SDK，无论访问方式封装成何种形式，其本质都是通过FunctionGraph提供的REST风格的API接口进行请求。FunctionGraph支持**Token认证和AK/SK认证**。

访问控制

IAM是提供权限管理的基础服务，您可以在IAM中创建不同的IAM用户，并配置策略来控制各个用户对云资源的访问范围。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

FunctionGraph服务支持通过IAM进行访问控制和权限管理，帮助用户安全的控制公有云资源的访问。具体FunctionGraph权限请参见**权限管理**。

- **IAM用户授权**：FunctionGraph支持为IAM用户授予不同级别的操作权限，实现细粒度的权限控制。不同IAM用户只能对被授权的函数进行访问和操作，确保资源的安全性。
- **云服务访问**：当函数需要访问其他云服务时，必须先为函数授予相应的访问权限。通过IAM身份策略，限制函数仅能访问其业务所需的必要资源，从而有效降低因权限滥用而带来的安全风险，保障云服务间交互的安全性。

8.4 数据保护技术

为了确保用户的数据（例如函数元数据等）不被未经过认证、授权的实体或者个人获取，FunctionGraph对数据的传输进行全程加密保护，以防止数据泄露，保证您的数据安全。

- 创建或更新函数时，可使用OBS地址或代码包上传新代码，FunctionGraph使用隔离的账号存储代码。初始化函数实例时，FunctionGraph申请临时下载地址，把代码下载到执行层，利用虚拟化隔离技术，限制函数实例只能访问自身代码。
- 函数的元数据和代码使用AES256加密存储，传输时均采用TLS 1.2及以上协议进行传输加密。
- 在数据传输过程中，所有的API请求调用和内部通信均采用TLS 1.2及以上协议进行传输加密。

8.5 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FunctionGraph的管理事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

通过云审计服务，您可以记录与FunctionGraph服务相关的操作事件，便于日后的查询、审计和回溯。相关内容请参见**云审计服务支持的FunctionGraph操作列表**。

日志

FunctionGraph实现了与云日志服务的对接。用户开通云日志服务后，可在监控页面或云日志服务中查询函数执行过程中的日志，帮助您更好的管理函数。具体请参见**函数日志**。

8.6 服务韧性

华为云数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划。

FunctionGraph的资源在多个分区部署，具有更高的可用性、容错性和可扩展性。

8.7 监控安全风险

FunctionGraph提供基于云监控服务CES的资源和操作监控能力，帮助用户监控账号下的函数，执行自动实时监控、告警和通知操作。用户可以掌握函数中的调用次数、错

误次数、运行时间（包括最大运行时间、最小运行时间、平均运行时间）、被拒绝次数、资源统计等信息。

关于FunctionGraph支持的监控指标，请参见**监控**。关于如何创建监控告警规则等内容，请参见**创建告警规则**。

8.8 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 8-2 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 8-3 资源中心

8.9 代码签名

为了保障用户的代码安全，防止代码文件损坏或被篡改导致代码不一致问题，保证被执行的函数代码为正确版本，当函数创建或修改代码时，FunctionGraph对用户的函数代码签名加密，为其生成代码签名，并存储在函数元信息内。

FunctionGraph在函数执行时，为当前执行的代码生成签名，然后将其与函数元信息内的代码签名进行对比，仅允许运行通过一致性校验的代码，校验未通过则不允许执行并返回错误。

8.10 数据面保障

负载均衡与网络安全防护

- 负载均衡优化可用性

  通过负载均衡技术实现流量分发，有效避免单点故障，大幅提升系统整体可用性，确保业务稳定运行。

- VPC环境确保网络隔离

  计算节点被安置在隔离的VPC环境中，与外部网络严格隔离，用户无法直接访问，保障网络的安全性和隔离性。

- 灵活配置网络

  函数默认开启公网访问权限，用户也可根据自身安全策略，配置访问特定VPC内资源。

调度安全防护

- 多集群配置增强容灾能力

  计算节点采用多集群多可用区的架构设计，支持资源的动态迁移。当某个可用区出现故障时，系统能够迅速将业务迁移到其他可用区，具备强大的容灾能力，保障业务的持续运行。

- 智能调度保障业务运行

  智能算法预测流量，并结合高速弹性扩容机制，快速响应突发流量。在资源接近耗尽时，系统会自动扩容，保障业务正常运行。

- 弹性与预留实例灵活配置

  函数实例分为弹性实例和预留实例两种类型。弹性实例能够根据业务负载的实时变化按需动态创建，业务空闲时自动释放，避免资源浪费。预留实例则由用户根据业务需求提前配置创建，且不会自动释放。用户可根据自身业务特点，自由设置弹性实例上限和预留实例数量，以满足不同业务场景的资源需求。

函数调用安全防护

- 同步调用

  直接对请求进行处理，不缓存请求信息，适用于对实时性要求极高的场景。

- 异步调用

  将请求缓存至消息队列中，确保请求至少被执行一次。通过账号级别或函数级别的队列隔离，有效防止不同用户之间的数据干扰。当调用失败时，系统默认重试3次，用户也可根据实际需求自定义重试次数，以灵活应对各种复杂场景。

运行时环境安全防护

- 漏洞修复和安全升级

  FunctionGraph负责定期对计算节点和函数实例进行漏洞扫描和修复，及时进行安全升级，确保运行时环境的安全性和稳定性。

- 不可变代码

  用户对代码的修改仅对后续新生成的实例生效，不会影响已经在运行的实例，确保代码的一致性和稳定性。

- 非持久化环境

  运行时环境的文件系统和内存会在实例释放时一同被释放，避免了数据残留带来的安全风险，同时也提高了资源的利用率。

- 异常信息收集

  运行时环境会自动收集函数执行过程中的异常信息和日志，帮助用户快速定位和解决问题，提高故障排查效率。

9 权限管理

如果您需要对FunctionGraph的函数资源，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公有云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制员工对云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望开发人员拥有FunctionGraph的使用权限，但是不希望开发人员拥有删除等高危操作的权限，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FunctionGraph，但是不允许删除的权限策略，控制开发人员对FunctionGraph资源的使用范围。

如果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FunctionGraph服务的其它功能。

IAM是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**《IAM产品介绍》**。

约束与限制

当添加了FunctionGraph FullAccess权限的子账号在创建触发器或使用其他功能时仍没有操作权限，是因为该服务或功能不支持细粒度鉴权，因此需要您单独添加对应服务或功能的Admin权限。具体详情如下：

- CTS、APIG、DIS当前不支持细粒度鉴权，需要添加对应admin权限。
- SMN目前部分局点已支持细粒度鉴权，如您遇到无法细粒度鉴权情况，则需要添加对应admin权限。
- IoTDA是新增加的触发器，FullAccess中缺少对应权限。您在创建该触发器时会提示需要创建委托并添加相应权限，创建委托需要您先添加iam: agencies:list，iam:agencies:createAgency 权限；
- TMS、DNS、BSS、CES、EG、DMS是新增加功能，FullAccess中缺少对应权限，需单独添加；

更多触发器及相关功能需要的权限，请参见**表9-2**所示。

企业项目授权后仍报权限不足的说明

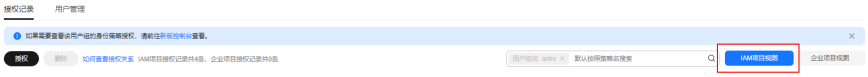
IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的

自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。关于IAM项目与企业项目的区别，详情请参见：**IAM和企业管理的区别**。

FunctionGraph当前仅函数资源接口支持企业项目方式授权，除函数资源外的部分接口仅支持IAM项目方式授权，因此针对仅支持IAM项目方式授权时需注意：

1. 授权时选择“IAM项目视图”。

   图 9-1 IAM 项目视图

2. 选择授权范围时，建议根据最小化授权原则，选择“指定区域项目资源”，具体请根据实际业务情况选择授权范围。

FunctionGraph 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，才能使得用户组中的用户获得策略定义的权限，这一过程称为授权。授权后，用户就可以基于策略对云服务进行操作。

FunctionGraph资源通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在各区域（如华北-北京1）对应的项目（cn-north-1）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FunctionGraph时，需要先切换至授权区域。

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。

如**表9-1**所示，包括了FunctionGraph的所有系统权限。

表 9-1 系统权限说明

系统角色/策略名称	描述	类别	依赖关系
FunctionGraph Administrator	函数工作流（FunctionGraph）管理员，具有管理函数、工作流、触发器以及调用函数的权限（该权限后期会下线，建议您不使用）	系统角色	Tenant Guest

系统角色/策略名称	描述	类别	依赖关系
FunctionGraph Invoker	函数工作流（FunctionGraph）调用者，具有查询函数、工作流、触发器以及调用函数的权限	系统角色	无
FunctionGraph FullAccess	函数工作流服务所有权限	系统策略	无
FunctionGraph ReadOnlyAccess	函数工作流服务只读权限	系统策略	无
FunctionGraph CommonOperations	函数工作流（FunctionGraph）调用者，具有查询函数和触发器，以及调用函数的权限	系统策略	无

表 9-2 触发器及相关功能的权限

触发器/服务功能	权限
APIG	apig:groups:get apig:groups:list apig:apis:create apig:apis:delete apig:apis:update apig:apis:publish apig:apis:list apig:apis:get apig:apis:offline apig:apps:list apig:envs:list
APIG专享版	apig:instances:get apig:instances:create apig:instances:update apig:instances:list apig:sharedInstance:operate
CTS	cts:notification:create cts:notification:delete cts:notification:update cts:operation:list cts:tracker:list cts:trace:list

触发器/服务功能	权限
DDS	dds:instance:get dds:instance:list
DIS	dis:streams:list
IoTDA	iotda:routingrules:create iotda:routingrules:delete iotda:routingrules:queryList iotda:routingrules:query iotda:routingactions:create iotda:routingactions:delete iotda:routingactions:query iotda:routingactions:queryList iotda:subscriptions:queryList iotda:rules:modifyStatus iotda:apps:queryList
LTS	lts:groups:create lts:groups:get lts:groups:list lts:groups:put lts:logstreams:delete lts:logstreams:list lts:topics:get lts:subscriptions:create lts:subscriptions:delete lts:subscriptions:put lts:structConfig:create lts:structConfig:get
OBS	obs:bucket:GetBucketLocation obs:bucket:GetBucketNotification obs:bucket:PutBucketNotification obs:bucket:ListBucket
SMN	smn:topic:list smn:topic:update
TMS	tms:predefineTags:list tms:tagValues:list

触发器/服务功能	权限
DNS	dns:recordset:create, dns:recordset:list, dns:recordset:update, dns:zone:create, dns:zone:delete, dns:zone:get, dns:zone:list
BSS	bss:bill:view bss:renewal:view
CES	ces:alarms:get ces:alarms:list ces:alarms:create
DMS	dms:instance:get
EG	eg:subscriptions:get eg:subscriptions:list eg:sources:list eg:sources:get eg:agency:create eg:subscriptions:create eg:subscriptions:delete eg:subscriptions:operate
分布式消息服务 Kafka版	dms:instance:list dms:instance:get dms:group:delete

表9-3列出了FunctionGraph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 9-3 常用操作与系统权限之间的关系

操作	FunctionGraph Invoker	FunctionGraph Administrator	FunctionGraph ReadOnly Access	FunctionGraph CommonOperations	FunctionGraph FullAccess
创建函数	×	√	×	×	√
查询函数	√	√	√	√	√
修改函数	×	√	×	×	√

操作	FunctionGraph Invoker	FunctionGraph Administrator	FunctionGraph ReadOnly Access	FunctionGraph CommonOperations	FunctionGraph FullAccess
删除函数	×	√	×	×	√
调用函数	√	√	×	√	√
查看函数日志	√	√	√	√	√
查看函数指标数据	√	√	√	√	√

相关链接

- IAM产品介绍。
- 创建用户组、用户并授予FunctionGraph权限。
- 策略支持的授权项。

10 基本概念

函数

函数是处理事件的自定义代码。

事件源

事件源是发布事件的公有云服务或自定义应用程序。

同步调用

同步调用指的是客户端请求需要明确等到响应结果，也就是说这样的请求必须得调用到用户的函数，并且等到调用完成才返回。

异步调用

异步调用是指客户端不关注请求调用的结果，服务端收到请求后将请求排队，排队成功后请求就返回，服务端在空闲的情况下会逐个处理排队的请求。

触发器

触发函数执行的事件。

函数流

用户通过在UI界面拖拽组件、配置组件和连接组件进行可视化编排，创建函数流任务，完成复杂场景的编排。

单实例多并发

单实例多并发是指单个实例可以同时处理的请求数量。

自定义镜像函数

用户直接打包上传容器镜像，由平台加载并启动运行。

自定义运行

自定义函数执行的脚本和文件。

函数日志

函数调用过程中产生的日志信息。

函数监控

函数执行过程中的监控信息。

函数版本

函数从开发、测试、生产过程中发布一个或多个版本，实现对函数代码的管理。对于发布的每个版本的函数、环境变量会另存为相应版本的快照，函数代码发布后，可以根据实际需要修改版本配置信息。

函数别名

用户可以创建别名，指向特定函数版本。别名的优势在于：如果需要回滚到之前的函数版本，则可以将相应别名指向该版本，不再需要修改代码信息。

函数别名支持绑定两个版本，一个对应版本和开启灰度版本，并且支持配置同一个别名下两个不同版本分流权重。

依赖包

依赖包管理模块统一管理用户所有的依赖包，用户可以通过本地上传和obs地址的形式上传依赖包，并为依赖包命名。

函数依赖包生成示例请参考**如何制作函数依赖包**。

调用链

调用链跟踪、记录业务的调用过程，可视化地还原业务请求在分布式系统中的执行路径和状态，用于性能及故障快速定界。

bootstrap 文件

bootstrap文件是HTTP函数的启动文件，HTTP函数仅支持读取bootstrap 作为启动文件名称，其它名称将无法正常启动服务。

11 与其他服务的关系

FunctionGraph服务与以下云服务的对接，实现相关功能，如**表11-1**所示。

表 11-1 对接服务

服务名称	实现功能
消息通知服务（SMN）	构建FunctionGraph函数来处理SMN的通知，相关内容请参考**消息通知服务用户指南**。
API网关（API Gateway）	通过HTTPS调用FunctionGraph函数，使用API Gateway自定义REST API和终端节点来实现。相关内容请参考**API网关用户指南**。
对象存储服务（OBS）	构建FunctionGraph函数来处理OBS存储桶事件，例如对象事件或删除事件。当用户将一张照片上传到存储桶时，OBS存储桶调用FunctionGraph函数，实现读取图像和创建照片缩略图。相关内容请参考**对象存储服务用户指南**。
数据接入服务（DIS）	构建FunctionGraph函数定期轮询DIS数据流中的新记录，例如网站点击流、财务交易记录、社交媒体源、IT日志和位置跟踪事件等。相关内容请参考**数据接入服务用户指南**。
云审计服务（CTS）	构建FunctionGraph函数，根据CTS云审计服务类型和操作订阅所需要的事件通知，由函数对日志中的关键信息进行分析和处理。 • 通过云审计服务，您可以记录与FunctionGraph服务相关的操作事件，便于日后的查询、审计和回溯。相关内容请参考**云审计服务支持的FunctionGraph操作列表**。 • 审计日志。开通云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。
云监控服务（CES）	FunctionGraph函数实现了与云监控服务对接，函数上报云监控服务的监控指标，用户可以通过云监控服务来查看函数产生的监控指标和告警信息。相关内容请参考**云监控服务用户指南**。 • 云监控支持的函数监控指标请参考**监控配置**。

服务名称	实现功能
虚拟私有云（VPC）	函数支持用户创建虚拟私有云（VPC）并访问自己VPC内的资源，同时支持通过SNAT方式绑定EIP访问外网。相关内容请参考**虚拟私有云用户指南**。

