函数工作流 FunctionGraph

产品介绍

文档版本 01

发布日期 2025-08-22

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。

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

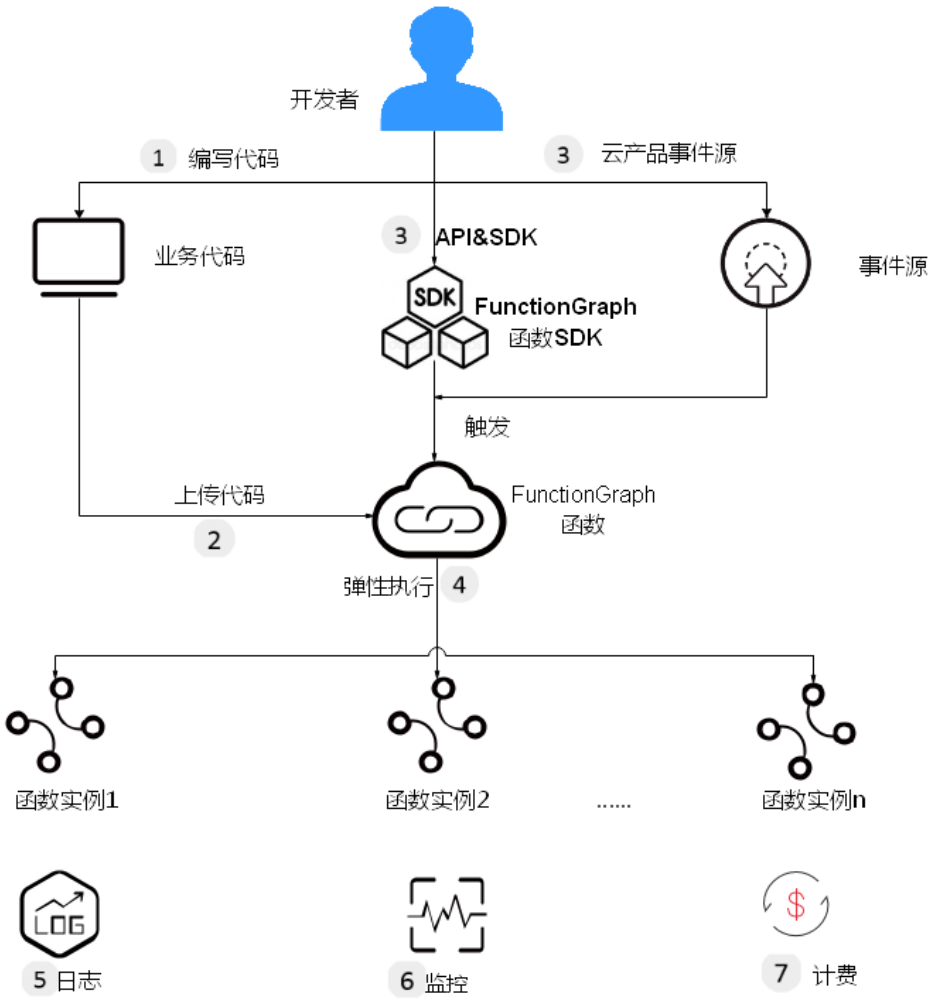
1 图解函数工作流服务

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和定制运行时语言，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，详情请参考**函数触发器**。

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LTS的对接，可查看函数运行日志信息，详情请参考**日志和监控**。

⑥查看监控

FunctionGraph函数实现了与应用运维管理服务AOM的对接，可查看图形化的函数监控信息，详情请参考**日志和监控**。

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，详情请参考**函数工作流计费概述**。

3 产品功能

函数管理

提供控制台管理函数。

- 函数支持Node.js、Python、Java、Go、C#、PHP运行时语言，同时支持用户定制运行时，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、20.15
Python	2.7、3.6、3.9、3.10、3.12
Java	8、11、17、21
Go	1.x
C#	.NET Core 2.1、.NET Core 3.1、.NET Core 6.0、.NET Core 8.0
PHP	7.3、8.3
Cangjie	1.0
定制运行时	-

- 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
Cangjie	不支持	支持	不支持	支持
定制运行时	支持	支持	不支持	支持

函数触发器

函数支持配置多种类型触发器，触发器调用方式如表3-3所示。

表 3-3 函数触发器的调用机制

触发器	调用方式
API网关服务（APIG专享版）	默认为同步调用，但可以修改为异步调用，具体配置方式请参考**配置函数的异步调用**。
API Connect（APIC）	默认为同步调用，但可以修改为异步调用，具体配置方式请参考**配置函数的异步调用**。
定时触发器（TIMER）	默认为同步调用。
云审计服务（CTS）	默认为异步调用，且不可修改。
文档数据库服务（DDS）	默认为异步调用，且不可修改。
数据接入服务（DIS）	默认为异步调用，且不可修改。
分布式消息服务 Kafka版（KAFKA）	默认为异步调用，且不可修改。
开源Kafka（OPENSOURCEKAFKA）	默认为异步调用，且不可修改。
分布式消息服务RabbitMQ版（RABBITMQ）	默认为异步调用，且不可修改。
云数据库 GeminiDB Mongo	默认为异步调用，且不可修改。
云日志服务（LTS）	默认为异步调用，且不可修改。

触发器	调用方式
消息通知服务（SMN）	默认为异步调用，且不可修改。
EventGrid触发器	默认为异步调用，且不可修改。

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 函数选型

6.1 函数类型选型

本文介绍函数工作流支持的函数类型的适用场景及差异，供您进行函数类型选型。

函数选型建议

为满足不同场景下的用户需求，函数工作流支持通过在线编写代码、上传代码文件或者使用容器镜像，创建事件函数和HTTP函数，且支持使用GPU计算资源。

在使用函数工作流时，可以根据业务场景和技术栈偏好，选择合适的函数类型和运行时。常见应用场景的函数选型建议请参考**表6-1**。

表 6-1 函数选型建议

应用场景	函数选型建议	说明
Web应用和API服务	使用代码创建**HTTP函数**	HTTP函数支持主流Web应用框架，可以通过浏览器访问，或由URL直接调用。
文件处理和数据流处理	结合**内置运行时**创建**事件函数**	事件函数可以配置事件触发，集成了多种华为云产品（如对象存储服务OBS、分布式消息服务 RabbitMQ 版、云日志服务LTS等）。
Chatbot和文生图等模型推理场景	结合**自定义镜像**创建**HTTP函数**并**启用GPU**	使用基于流行AI项目（如Stable Diffusion、ComfyUI、Ollama等）的容器镜像创建HTTP函数，启用GPU快速构建AI模型推理服务。
定时任务和音视频转码等异步任务场景	结合**内置运行时**创建**事件函数**	事件函数可以配置事件触发，能够通过特定事件或定时触发来调用关联函数。

函数类型选型分析

关于事件函数与HTTP函数的具体分析，请参考**表6-2**。

表 6-2 函数类型选型分析

对比项	事件函数	HTTP函数
功能	用于处理文件和数据流，可以通过各类云产品的事件触发（如**基于EG的OBS应用事件源触发器**、**Kafka触发器**、**LTS触发器**等），以及用于处理异步请求，能够追踪并保存每个异步调用的状态。	支持流行的Web应用框架和AI流行项目，可以通过浏览器访问，或通过URL调用。
适用场景	• 云产品集成： OBS实时文件处理、LTS日志加工等。 • ETL数据加工：数据库数据清洗、消息队列处理等。 • 常规任务：定时任务、周期任务、脚本任务等。 • 多媒体处理：音视频转码、直播录制、图片加工等。	• 快速构建流行Web框架应用：Express、Flask等。 • 快速构建AI模型推理服务：如Stable Diffusion、ComfyUI、Ollama等。 • 迁移已有的应用：HTML5网站、REST API、BFF、移动APP、小程序、游戏结算等。
运行环境	推荐使用**内置运行时**。	推荐使用**定制运行时**或**自定义镜像**。

函数运行环境选型分析

关于函数运行环境的具体分析，请参考**表6-3**。

表 6-3 函数运行环境选型分析

对比项	内置运行时	定制运行时	自定义镜像
开发流程	根据函数工作流定义的函数执行入口编写请求处理程序。	基于Web应用框架模板开发应用，通过公网访问地址即时看到结果。	将自定义镜像上传至SWR然后使用镜像，或者使用SWR中已有的镜像。
支持的实例类型	CPU实例	CPU实例和GPU实例	CPU实例和GPU实例
单实例多并发	不支持	支持	支持
冷启动	最快。 代码包中不包含运行时，因此冷启动最快。	较快。 代码包是一个HTTP Server程序，体积较大，但不需要拉取SWR容器镜像，因此冷启动会较快。	较慢。 需要拉取镜像，因此冷启动较慢。
代码文件大小限制	代码包大小不超过100MB或500MB，具体请参见**代码部署包大小限制说明**。		未解压的镜像大小不超过10 GB。

对比项	内置运行时	定制运行时	自定义镜像
代码文件格式	ZIP、JAR（Java）		容器镜像
支持的编程语言	Node.js、Python、PHP、Java、C#、Go	无限制	无限制

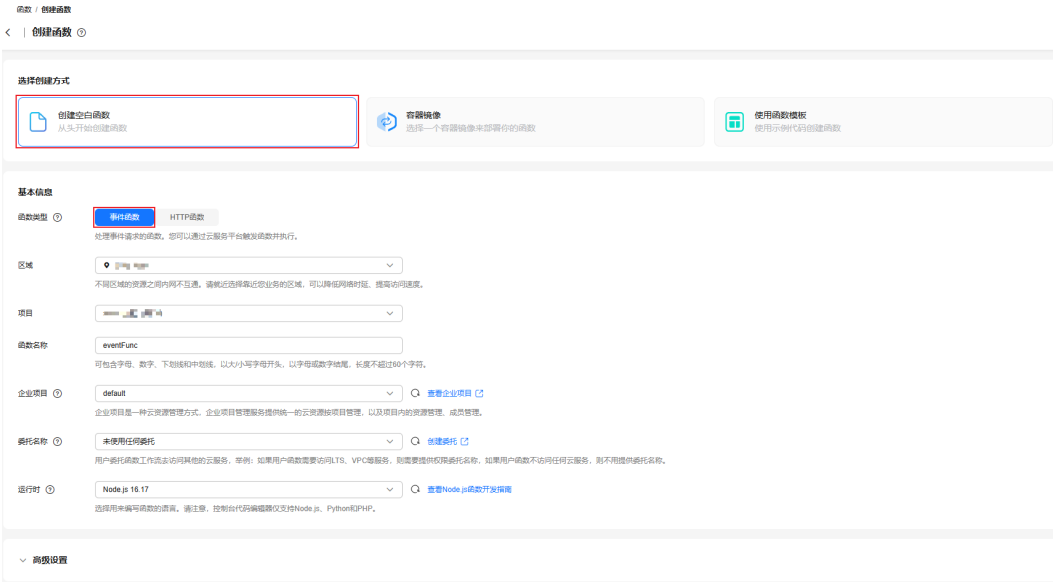
通过控制台创建函数

通过函数工作流控制台，支持创建以下函数。

事件函数

如果想通过特定事件或定时触发来调用关联函数，可通过函数工作流控制台，如图6-1所示创建事件函数，推荐选择**内置运行时**作为运行环境。具体操作步骤，请参考**创建事件函数**。

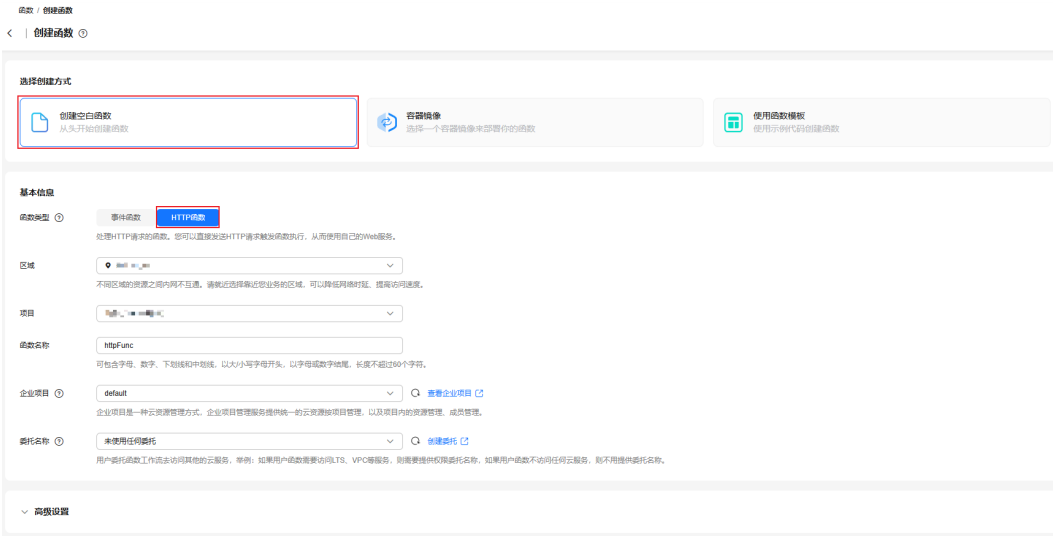
图 6-1 创建事件函数



HTTP 函数

如果想基于各个语言的流行框架编写程序，可通过函数工作流控制台如图6-2所示创建HTTP函数，推荐选择**定制运行时**作为运行环境。具体操作步骤，请参考**创建HTTP函数**。

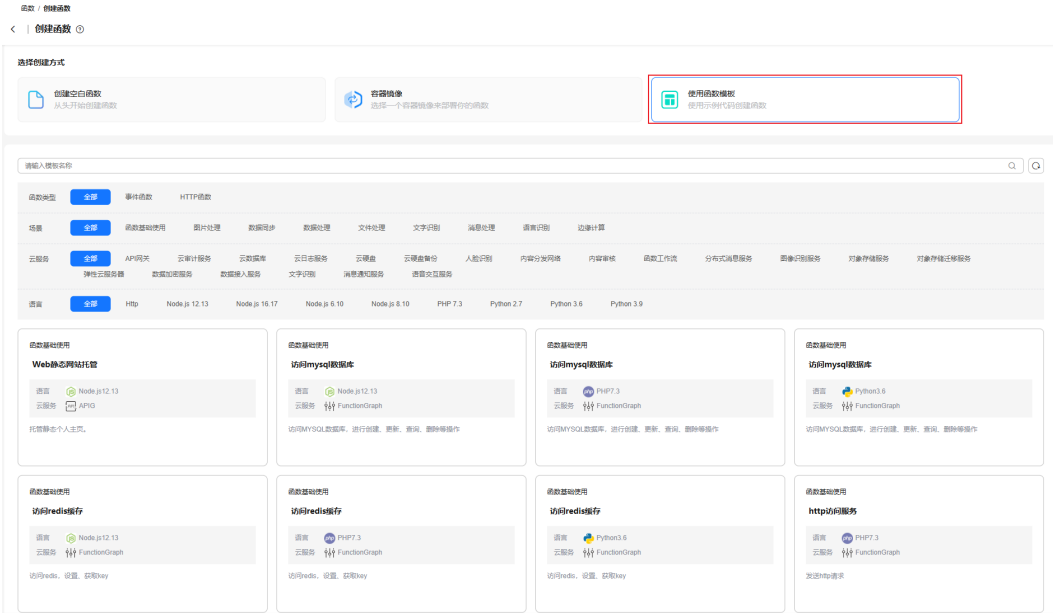
图 6-2 创建 HTTP 函数



模板函数

FunctionGraph提供多种场景的函数模板，在使用函数模板创建函数时，能够实现代码与环境变量的自动填充，快速构建函数应用。如您的需求可由函数模板满足，如图6-3所示，可以选择**使用函数模板创建函数**。

图 6-3 使用模板创建函数



6.2 函数存储选型

本文介绍函数工作流支持的存储类型的适用场景及差异，供您进行函数存储选型。

函数存储选型分析

为了满足业务存储和访问文件的诉求，函数工作流提供丰富的存储类型，包括弹性云服务器ECS、高性能弹性文件服务SFS Turbo、对象存储服务OBS、临时存储和函数依赖包。具体的存储选型对比分析请参考**表6-4**。

表 6-4 函数存储选型分析

对比项	弹性云服务器 ECS	高性能弹性文件服务 SFS Turbo	对象存储服务 OBS	临时存储	函数依赖包
适用场景	日志、业务文件存储	日志、业务文件存储	日志、业务文件存储	业务产生的临时文件	公共依赖库、运行时环境及函数扩展等发布与部署
最大空间	可扩展	弹性	弹性	默认情况下为512MB，可以自行调整为最大10GB。	300 MB
持久性	持久	持久	持久	临时存储	持久
调用间共享	是	是	是	否	是
存储内容	可写	可写	可写	可写	不可写
存储类型	文件系统	文件系统	对象	文件系统	代码依赖归档
事件源集成	否	否	是	否	否
函数访问速度	较快	较快	快	最快	快
计费	ECS计费概述	SFS Turbo计费概述	OBS计费概述	硬盘规格≤512 MB时免费，具体见计费项	不计费

存储类型介绍

函数工作流支持的存储类型具体介绍如下。

弹性云服务器 ECS

弹性云服务器（Elastic Cloud Server，ECS）可以通过启动NFS文件服务对外提供安全、高性能、高可靠、简单易用的文件存储服务。

华为云函数工作流支持与弹性云服务器ECS无缝集成，支持为函数配置挂载ECS的共享路径。配置成功后，函数可以像访问本地文件系统一样访问指定的ECS共享路径。

使用ECS作为函数挂载的优势如下：

- 可以将临时文件存储到ECS共享路径中，临时文件大小不受实例本地磁盘空间限制。
- 多个函数可以共用一个ECS共享路径，实现文件共享。

具体挂载操作，请参见**扩展函数的存储空间**。

高性能弹性文件服务 SFS Turbo

高性能弹性文件服务（Scalable File Service Turbo，SFS Turbo）提供按需扩展的高性能文件存储（NAS），可为云上多个弹性云服务器（ECS）、容器（CCE&CCI）、裸金属服务器（BMS）提供共享访问。

华为云函数工作流支持与高性能弹性文件服务SFS Turbo无缝集成，支持为函数挂载SFS Turbo文件系统。配置成功后，函数可以像访问本地文件系统一样访问指定的文件系统。

使用SFS Turbo作为函数挂载的优势如下：

- 可以将临时文件存储到SFS Turbo文件系统中，临时文件大小不受实例本地磁盘空间限制。
- 多个函数可以共用一个SFS Turbo文件系统，实现文件共享。

具体挂载操作，请参见**扩展函数的存储空间**。

对象存储服务 OBS

对象存储服务（Object Storage Service，OBS）提供海量、安全、高可靠且低成本的数据存储能力，支持存储任意类型和大小的数据。适用于企业备份、归档、视频点播、视频监控等多种数据存储场景。

函数工作流与OBS能够通过基于EventGrid（EG）的OBS事件源触发器实现无缝集成，可以编写函数对OBS事件进行自定义处理，例如能够调用多种函数处理图像或音频数据，并将处理结果写入不同类型存储服务中。您只需专注于编写函数逻辑，系统将以实时、可靠的大规模并行方式处理海量数据。

具体使用操作，请参见**使用EventGrid触发器（OBS应用事件源）**。也支持在函数代码中，使用OBS对应语言的SDK工具实现对OBS的读写处理。

临时存储

函数工作流提供两种临时存储规格，分别为512MB和10GB。

临时存储空间的生命周期与底层执行函数的实例相同。若持续有请求，实例将保持存在，因此先前存储于磁盘的数据仍将保留。若函数在长时间内未收到请求，系统将回收该实例，此时磁盘上的数据将随之消失。

函数依赖包

函数依赖包包含支持函数业务代码运行的公共库，可以将代码所需的公共库封装成依赖包进行单独管理，便于多函数共享，同时也能有效缩减函数代码在部署与更新过程中的体积。

关于函数依赖包的操作和使用限制，请参见**函数依赖包**。

7 函数实例类型与使用模式

本文为您介绍函数CPU实例和GPU实例的实例模式、计费方式及实例规格。

实例类型

函数实例有以下两种实例类型：

- CPU实例：函数工作流的基本实例，适用于突发流量和计算密集等场景。
- GPU实例：提供基于Turing架构的GPU实例，适用于音视频、AI人工智能和图像处理等场景。在各场景中，不同业务负载通过GPU硬件加速，以提升业务处理效率。

  GPU实例仅支持通过容器镜像和定制运行时方式部署，仅支持在“华东-上海一”区域下部署。

实例模式

CPU实例和GPU实例均支持两种实例模式：按量模式和预留模式。两种实例模式说明如下：

按量模式

按量模式是指函数实例的分配和释放完全由函数工作流系统负责，函数工作流会根据函数的调用量自动调整实例数量：在调用请求增加时创建实例，减少后销毁实例。

在函数使用过程中，请求会自动触发函数实例的创建，若实例在一段时间内（通常为1分钟）不处理请求，则自动销毁。初次调用时，需等待实例冷启动。

约束与限制：

单个华为云账号（子账号）在单个区域内总实例数默认限制为1000。如果业务有更大的实例数需求，请**提交工单**申请。

计费方式：

按量模式下，函数执行时长的计量从请求触发函数执行开始，直至请求处理完成结束。该模式下，单个实例可处理单个请求（单实例单并发），或根据配置支持并发处理多个请求（单实例多并发）。执行时长说明请参见**表7-1**，具体配置方法请参见**配置函数的并发处理**。

当无函数调用时，系统不会分配计算资源，因此不产生费用；仅在函数被实际调用并执行时，才会根据资源使用情况计费。详细的产品定价与计费规则，请参见**计费概述**。

表 7-1 请求方式执行时长说明

请求方式	执行时长说明	示例
单实例单并发	一个实例执行一个请求时，执行时长的计量从请求到达实例开始，至请求执行完毕结束。	• 若请求在 00:00:00 到达，于 00:00:05 结束，则计费时长为5秒。 • 若同时有三个请求到达并各自耗时5秒，则总计费时长为 3×5=15秒。
单实例多并发	一个实例并发执行多个请求时，执行时长的计量从第一个请求到达实例开始，至最后一个请求执行完毕结束，可以复用资源节省费用。	第一个请求在 00:00:00 到达，于 00:00:05 结束，最后一个请求在 00:00:03 到达，于 00:00:08 结束，他们会在同一个实例中执行，则总计费时长为8秒。

预留模式

预留模式通过用户自主管理函数实例的生命周期，实现对计算资源的灵活控制。当用户为函数配置预留实例后，FunctionGraph在接收到调用请求时将优先调度至常驻的预留实例进行处理。当业务流量超出预留资源承载能力时，系统将自动触发弹性扩缩容机制，通过按量实例动态分配执行环境以保障服务连续性。

该模式下，预留实例在创建阶段即完成函数代码、依赖组件的预加载，并执行初始化入口函数，从而构建出持久化的执行环境。这种常驻机制可显著降低冷启动带来的延迟问题，因此如果希望降低冷启动时间，预留模式是最佳方案。建议根据业务资源预算选择**配置固定数量的预留实例策略**，根据波峰波谷特性**配置定时伸缩的预留实例策略**、**按指标伸缩的预留实例策略**和**智能伸缩的预留实例策略**。

注意事项：

需注意不要依赖预留实例本身的初始化入口函数去执行一次性业务，以确保服务的稳定性和可靠性。

计费方式：

请参考计费项中**计费说明**的执行时间费用（预留实例）部分和**预留实例计费规则**。

实例规格

- CPU实例

  CPU实例包含以下实例规格，可以根据业务需求选择不同配置的实例。

表 7-2 CPU 实例规格

内存规格	代码包大小上限	函数执行时长上限	磁盘大小上限
128~32768 MB 取值说明：必须为64的倍数。	• ZIP文件：解压后原始代码大小为1.5GB。 • 上传OBS桶中的文件：最大可上传300MB压缩后的代码包。	259200s 如需调用执行时间超过900秒的函数，请使用异步调用的方式。	取值说明：可选512MB或10GB，默认值为512MB。

- GPU实例

  GPU实例包含以下实例规格，可以根据业务需求选择不同配置的实例。

表 7-3 GPU 实例规格

显卡类型	整卡显存	整卡算力（TFLOPS）		可选切分规格		是否支持按量模式	是否支持普通预留模式	是否支持闲置预留模式
NVIDIA T4	16GB	**FP16算力**	**FP32算力**	**显存（MB）**	**内存规格（MB）**	是	是	是
		65	8	1024~16384（对应1GB~16GB） 取值说明：必须为1024MB的倍数。	128~32768 取值说明：必须为64的倍数。			

8 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 8-1 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 8-2 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 8-3 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 8-4 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。

9 安全

9.1 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9-1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 9-1 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9-1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。

用户身份认证凭据保护

用户通过身份凭据，如IAM AK、SK、Token等，访问云服务。若凭据泄露，将无法保障业务安全。用户应使用IAM遵循最小权限原则授权，以减小身份凭据泄露时遭受攻击的影响范围。

用户函数代码安全

用户代码和私有依赖包是用户的核心资产，用户需确保代码的可靠性和安全性，避免在代码中嵌入敏感信息，如账号、密码，访问密钥（AK/SK），令牌（Token）等，并确保日志中不记录敏感信息，以防敏感信息泄露。

用户函数配置安全

- **使用加密环境变量**

  用户代码中的敏感信息配置可通过**加密环境变量**传递，如访问其他云服务的AK/SK，访问数据库的密码等，FunctionGraph会对加密环境变量进行加密存储，避免敏感信息泄露。

  图 9-2 加密环境变量

- **函数外部网络访问配置**

  函数访问公网：函数默认允许公网访问，采用公网访问时所有租户共享带宽，存在遭受外部网络攻击的风险。用户可以**配置VPC**，通过用户VPC访问公网，独享网络带宽。

  函数访问VPC：当用户需要访问云服务VPC内的资源，如数据库、缓存服务等，建议配置VPC，以避免敏感信息泄露。

- **委托权限最小化**

  用户应根据实际需求为函数**函数配置委托**和执行授权（访问其他华为云服务，如ECS、OBS等所需的授权），并设定恰当的权限，授权权限需遵循**最小使用原则**，以降低授权Token泄露引发的安全风险。

9.2 资产识别与管理

在函数的整个生命周期中，FunctionGraph提供安全的运行环境，用户需结合FunctionGraph提供的安全机制确保代码、依赖包及配置的安全。

运行环境安全

FunctionGraph服务提供用户代码执行所需的计算节点和函数实例。该服务基于用户调用量综合评估后，提供有效的算力，同时确保节点的可用性和安全性。

计算节点安全

计算节点提供以下华为云标准的安全防护能力，详情请参考**《华为云安全白皮书》**。

- **多AZ多集群容灾**：一个region的计算节点部署在多个AZ（可用区）、多个集群，具备可用区容灾能力。
- **独立的VPC环境**：计算节点位于独立隔离的VPC中，用户无法直接访问计算节点。
- **主机安全防护**：计算节点使用华为云**企业主机安全HSS服务**，提供漏洞检测，安全检测和防御，并与华为云安全部门协作，提供快速感知与处置能力。

- **漏洞修复或安全升级：**FunctionGraph负责计算节点的漏洞修复及安全升级，且升级过程对用户透明。当存在不兼容风险时，将以公告或短信形式通知客户并提供适配方案，确保用户业务平滑迁移。

函数实例安全

函数实例提供函数级隔离能力，每个实例仅允许一个函数运行。

- **网络隔离：**函数实例间及函数实例与节点间均不可直接访问。根据用户的**配置**，函数实例可选择是否访问公网或用户VPC网络。
- **函数实例冻结：**当检测到恶意租户攻击时，FunctionGraph可即时冻结并隔离恶意用户函数实例，确保运行环境安全。
- **漏洞修复和安全升级：**FunctionGraph负责函数实例的漏洞修复及安全升级，且升级过程对用户透明。当存在不兼容风险时，将以公告或短信形式通知客户并提供适配方案，确保用户业务平滑迁移。
- **运行时停止维护：**随社区停止维护，FunctionGraph提供的运行时将逐步进入淘汰流程，禁止用户使用已停止维护的运行时创建函数。建议客户尽快迁移现有函数至新运行时，FunctionGraph不保证已停止支持的运行时版本能够持续正常运行。

用户代码安全

- **代码分享和下载：**FunctionGraph可以为用户提供临时代码及下载地址，并设置有效期，用户应避免临时下载地址泄露，以降低代码或库泄露的风险。
- **敏感信息防泄露：**用户应避免在代码或依赖包中明文记录敏感信息，例如访问密钥（AK）、安全密钥（SK）、数据库密码等；用户代码日志中应避免打印令牌（token）、密码等敏感信息，以防敏感信息泄露。
- **代码无漏洞：**用户需确保代码、库和依赖包安全性，及时识别、修复漏洞并更新函数。防止因用户代码漏洞引发攻击，从而影响业务安全。

华为云为FunctionGraph提供了多个安全云服务，可增强代码扫、威胁分析等安全能力。

表 9-1 华为云安全云服务说明

华为云服务	说明
代码检查服务 CodeArts Check	支持对FunctionGraph的代码进行多维度安全扫描，覆盖代码风格、质量及安全问题。其核心能力包括： • 自研检查引擎：支持C/C++、Java、Python等主流语言，可识别安全漏洞（如缓冲区溢出、未授权访问、加密问题）和代码规范问题。 • 安全标准支持：集成ISO 5055、CWE、OWASP TOP 10等标准，结合华为30年研发经验的内置规范（如《华为C/C++编程规范》），确保代码符合安全要求。 • 大规模扫描能力：日均百亿级扫描能力，支持弹性调度和容灾机制，适用于FunctionGraph的代码库全量检查。

华为云服务	说明
安全云脑 SecMaster	安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。 通过分析FunctionGraph相关云服务（如OBS、VPC）的日志数据，实时检测恶意行为。 • 多维度日志分析：采集IAM、DNS、CTS等日志，利用AI引擎和威胁情报识别暴力破解和渗透攻击等威胁。 • 告警与响应：生成威胁告警并输出统计结果，帮助您及时处理潜在风险，保障服务稳定。

可结合CodeArts Check实现代码侧全流程防护，同时通过SecMaster监控运行时威胁，构建FunctionGraph的安全增强体系。

用户配置安全

- **敏感信息保护：**当用户代码或配置中包含敏感信息时，强烈建议使用加密环境变量，以避免在用户界面或API返回结果中出现明文展示，从而预防敏感信息泄露。
- **委托权限最小化：**在配置触发器、VPC访问、自定义镜像、磁盘挂载等场景中，FunctionGraph需与其他云服务协同作业，需要创建云服务委托，确保FunctionGraph具备代表您执行部分资源运维工作的权限。配置委托时应遵循权限最小化原则，能够有效降低委托Token泄露时攻击的影响范围。
- **使用KMS动态加解密**（华为云数据加密服务DEW）：若需在函数运行时解密敏感数据（如数据库密码、API密钥），可通过KMS SDK动态操作密钥。用户可以将加解密密钥托管在KMS，并在IAM服务为函数创建委托授权FunctionGraph访问KMS（授权满足最小化使用原则），授权策略如下所示：

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "kms:Decrypt",
 "Resource": "arn:huaweicloud:kms:REGION:ACCOUNT_ID:keyring/kms-ring-123456/key/kms-key-123456"
 }
 ]
 }
```

然后在代码中添加KMS SDK代码片段以获取密钥，从而对敏感数据进行加解密操作。如下以python代码片段为例。

```
from huaweicloudsdkkms import KmsClient, models

def decrypt_data():
# 初始化KMS客户端
kms_client = KmsClient(
secret_id=os.getenv('KMS_SECRET_ID'),
secret_key=os.getenv('KMS_SECRET_KEY'),
region_name="cn-north-4"
)

# 解密数据
decrypt_request = models.DecryptRequest(
key_id="kms-key-123456",
```

```
ciphertext=b"encrypted_data_base64",
encryption_algorithm="AES_256_CBC"
)
response = kms_client.decrypt(decrypt_request)
return response.plaintext.decode('utf-8')
```

9.3 身份认证与访问控制

FunctionGraph基于华为云**统一身份认证服务IAM**实现用户身份认证和对华为云资源进行精细的访问控制。

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

FunctionGraph服务支持通过IAM进行访问控制和精细的权限管理，能够帮助用户安全控制公有云资源的访问。详情请参见**权限管理**。

用户授权时尽量满足**最小使用权限原则**，可有效降低凭据泄露时的攻击范围，最小化业务影响。

- 事件源配置：用户需为事件源创建触发器，并为触发器授予相应的执行权限，以实现函数的触发。
- 云服务访问：用户访问其他云服务，如对象存储OBS、日志服务LTS时，需授予相应的访问权限。
- IAM用户（子账号）授权：FunctionGraph支持通过IAM服务为IAM用户（子账号）赋予不同的函数操作权限。

9.4 数据保护技术

为了确保用户的数据（例如代码、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。

数据保护技术

FunctionGraph中使用的数据保护技术如**表9-2**所示。

表 9-2 数据保护技术说明

数据保护技术	说明
加密传输	所有的API请求调用和内部通信均通过TLS 1.2及以上协议进行加密传输。
加密存储	函数敏感信息配置和用户代码缓存使用AES算法加密存储，使用时解密。

数据保护技术	说明
其他数据保护技术	• 用户创建函数或依赖包时，用户代码存储在私有OBS桶，并为每个对象设置ACL控制，确保仅其租户能够读写，从而有效隔离其他租户的访问。 • 用户自定义镜像创建函数时，镜像存储在用户本人的SWR，仅用户自身账号可下载镜像。 • 用户函数实例是函数级别的，不同函数使用不同的实例，确保用户数据的严格隔离。 • 用户停止调用函数后，后台将在指定时间后回收函数实例，防止实例复用引发的数据泄露。

9.5 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，帮助您更好地管理函数。具体请参见**函数日志**。

9.6 服务韧性

资源分区部署

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。

FunctionGraph 架构功能

在华为云基础架构之上，FunctionGraph还提供了多种功能，以支持数据故障恢复能力和备份需求。

版本控制：建议在FunctionGraph中使用版本控制，以便在开发过程中保存函数的代码和配置。通过与别名配合，可以使用版本控制执行蓝/绿和滚动部署。详细信息请参阅**配置函数版本**。

弹性：当函数在处理前一个请求时收到新请求，FunctionGraph会启动另一个函数实例来处理增加的负载。FunctionGraph会弹性伸缩，以处理每个区域最大1000个并发执行，配额可根据需要调整。详细信息请参阅**函数并发配置**。

高可用性：FunctionGraph会在多个可用区中运行函数，确保在某一区域服务中断时仍能处理事件。如果将函数配置为连接至账户中的VPC，请指定多个可用区中的子网以确保高可用性。详细信息请参阅**配置函数访问VPC**。

重试：对于异步调用和由其他服务触发的触发器，FunctionGraph在遇到错误时会自动重试（每次重试有延迟）。对于同步调用，函数的其他客户端和华为云服务负责执行重试。详细信息请参阅**配置函数异步**。

死信队列：对于异步调用，如果所有重试均失败，可以配置FunctionGraph向死信队列发送请求。死信队列会接收事件以进行故障排除或重新处理（白名单限制，如需使用请**提交工单**）。

9.7 监控安全风险

- FunctionGraph基于云监控服务CES提供资源与操作监控能力，帮助用户监控其账号下的函数，实现自动实时监控、告警及通知。用户能够了解函数的调用次数、错误次数、运行时间（包括最大、最小和平均运行时间）、被拒绝次数及资源统计等信息。
- 云审计服务（CTS）提供多种云资源操作记录的收集、存储和查询功能，支持安全分析、合规审计、资源跟踪、问题回溯及定位等应用场景。使用CTS能对函数资源操作的全生命周期进行追踪，实时告警函数重要配置变更，迅速感知并追踪函数资源动态。
- 云防火墙（CFW）在网络层提供威胁防护，集成了IPS/IDS功能，支持基于流量分析的DDoS攻击防护、恶意IP地址库自动拦截及网络访问控制策略的自动优化建议。当用户配置VPC并访问公网时，可通过连接CFW服务增强外部网络安全防护。

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**。

9.8 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 9-3 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 9-4 资源中心

9.9 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。

9.10 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。

10 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，可以帮助您安全地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10-2**所示。

企业项目授权后仍报权限不足的说明

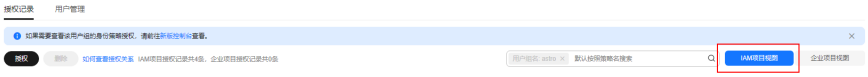
IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的

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 10-1 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10-1**所示，包括了FunctionGraph的所有系统权限。

表 10-1 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 10-2 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10-3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 10-3 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 ReadOnlyAccess	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。

11 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。

运行时

运行时（Runtime）为相应的编程语言提供执行环境，用于传递函数的调用事件、上下文信息和响应。

FunctionGraph当前支持Node.js、Python、Java、Go、C#、PHP、Cangjie以及定制运行时。

关于函数运行时的更多信息请参见**函数运行时**。

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。

关于函数调用的更多信息请参见**调用函数**。

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。

关于函数调用的更多信息请参见**调用函数**。

触发器

触发函数执行的事件。部分其他华为云服务可以使用触发器，实现在指定云服务的事件发生时，直接触发FunctionGraph的函数执行。

关于触发器的更多信息请参见**FunctionGraph支持的触发事件**。

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。

关于函数流的更多信息请参见**函数流管理**。

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

依赖包包含支持函数业务代码运行的公共库，可以将代码所需的公共库封装成依赖包进行单独管理，便于多函数共享，同时也能有效缩减函数代码在部署与更新过程中的体积。

关于函数依赖包的更多信息请参见**配置函数依赖包**。

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。

12 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12-1**所示。

表 12-1 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**。
分布式消息服务（DMS）	将FunctionGraph函数配置为自动轮询DMS消息队列并处理任何新消息，相关内容请参考**分布式消息服务用户指南**。
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**。
应用运维管理（AOM）	FunctionGraph函数实现了与应用运维管理服务AOM的对接，可在控制台界面查看图形化的函数监控信息。相关内容请参考**查看FunctionGraph的监控数据**。