API 中心

产品介绍

文档版本	08
发布日期	2023-09-27

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2023。 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


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

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

1 图解 API 中心

版权所有 © 华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司

2 什么是 API 中心

API（Application Programing Interface，应用程序接口）是一些预先定义的函数，目的是提供应用程序与开发人员基于软件或硬件得以访问一组例程的能力，而又无需访问源码或理解内部工作机制的细节。API中心是为API开发者和应用开发者构建的海量API的汇聚运营平台。帮助API开发者高效便捷地分享和开放API，支持应用开发者快速查找所需API并进行应用开发和集成。

此外，通过对接集成API工具、华为云商店、华为云集成工作台、低代码平台等华为云或生态伙伴相关服务或产品，为API开发者提供高效协同、自动化的API生产工具，并支持高价值API商业售卖；为应用开发者提供多场景、低门槛的低代码应用开发环境和开箱即用的API。

通过统一汇聚和持续运营，华为云API中心贯通并粘合API生产、API开放和API消费，促进API供需匹配，形成API生产、消费、再生产的良性循环，与伙伴和开发者共建繁荣API经济。

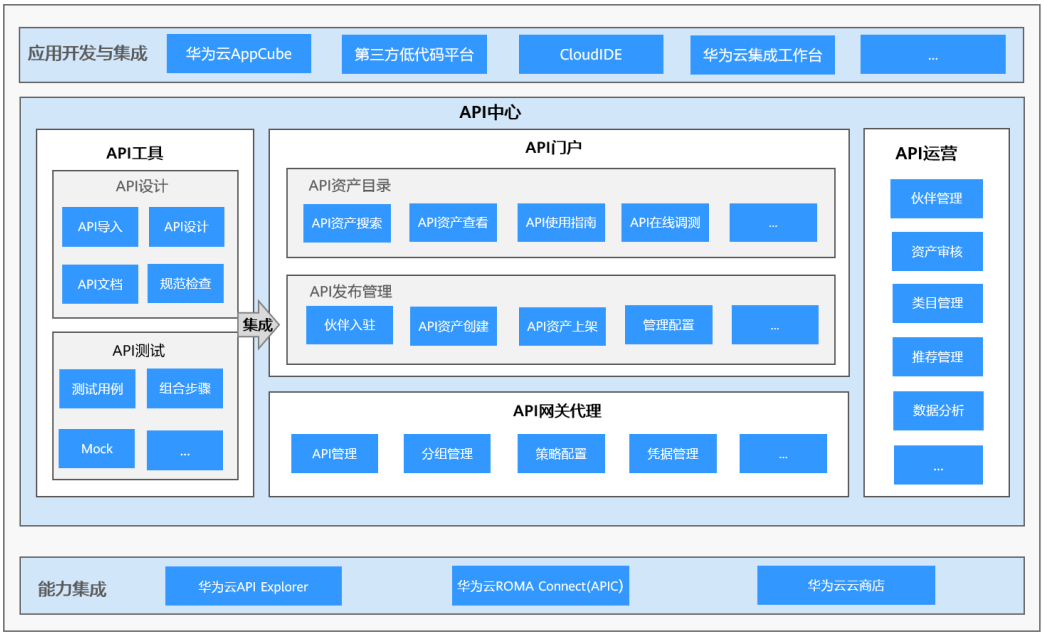
为什么选择 API 中心

- 覆盖API生产、API开放、API消费全场景，一站式体验。
- 引入自动化的API工具，帮助API开发者高效设计/开发/测试API。
- 通过智能搜索和推荐，帮助应用开发者从海量API中快速找到所需API。
- 体系化、精细化的数据分析，帮助伙伴驱动API业务创新和发展。

版权所有 © 华为云计算技术有限公司

产品架构

图 2-1 API 中心产品架构



API中心主要包括API工具，API门户，API网关代理，API运营四个产品模块：

- **API工具**

  API中心通过对接集成API开发工具，为API开发者提供简单易用的API工具，帮助开发者高效地设计、测试API。

- **API门户**

  API中心构建面向广大开发者的统一API门户。API开发者可以申请入驻成为API中心的伙伴服务商，并在管理控制台发布并开放API。应用开发者可通过API门户的资产目录便捷高效地查找和获取API，并进行调测、试用。

- **API网关代理**

  API中心的网关代理模块提供API管理，分组管理，策略配置，凭据管理等能力。帮助伙伴服务商对外开放API服务，为API数据分析提供支撑。

- **API运营**

  API中心为平台运营人员提供灵活高效的运营管理能力。通过平台运营构建友好的、可持续发展的生态环境，促进API供需匹配，与伙伴/开发者共建繁荣API经济。

在能力集成方面：

- API中心对接集成华为云API Explorer，并将其作为API中心的API调试功能模块，支持开发者在API中心直接调测、试用API。
- API中心聚集API开发者和应用开发者，并汇聚技术开放和商业售卖的所有API。其中，商业售卖的API，基于华为云云商店实现交易和变现。
- ROMA Connect的APIC模块作为底层组件为API中心提供网关实例资源，API中心的网关代理对外提供逻辑多租能力，构建面向生态伙伴/开发者的API生态网关。

版权所有 © 华为云计算技术有限公司

访问方式

API中心分为API门户和管理控制台。

- API门户的访问方式：通过浏览器（推荐Chrome）直接访问**API中心门户网站**，支持用户免登录情况下查看和搜索API。
- 管理控制台的访问方式：通过浏览器（推荐Chrome）使用**API中心管理控制台**方式进行API资产管理、API注册到网关等。

版权所有 © 华为云计算技术有限公司

3 产品优势

API 生产便捷高效

通过对接集成，API中心为开发者引入API生产工具：API Arts。

- API设计、测试一站式高效协同，API数据自动同步。
- API设计与文档实时同步，设计即文档。
- API测试与设计同源，设计示例一键导入测试步骤。

API 开放简单体验

一键上架：API生产工具中的API资产可以一键上架到API门户，实现开放分享。

API 消费快速匹配

- 支持智能搜索和推荐，缩短应用开发者和API资产的触达路径，帮助应用开发者快速找到所需API。
- 支持在线调测，快速试用和体验API。
- 与华为云集成工作台对接集成，支持API快速生成连接器，并用于SaaS开发和集成。

版权所有 © 华为云计算技术有限公司

4 应用场景

API 设计开发

当前面临的主要问题

- 缺少高效的生产作业平台。
- 多系统数据不互通、学习成本高、数据一致性困难、效率低、无法团队协作。

API中心解决方案

API中心从华为云或生态伙伴选型轻量化、具备便捷开发体验（高效协同、自动化等）的API工具，并对接集成引入到API中心的API工具库，供API开发者使用。

API 技术开放

当前面临的主要问题

- 业界海量API碎片化分布，缺少统一的汇聚平台展示API。
- 应用开发者缺少行业价值API的获取途径，不清楚哪些API可用。

API中心解决方案

API中心构建统一汇聚和展示千行百业海量API的开发者门户，为应用开发者提供统一的API搜索查找入口，并通过智能搜索和推荐，帮助开发者快速找到所需API。

API 商业变现

当前面临的主要问题

- API商业变现方式不够灵活。
- 缺少多维度的数据分析支撑。

API中心解决方案

API中心协同华为云云商店为API构建灵活多样的商业闭环路径，并提供API调用次数、API调用者等数据分析能力。

- 直接变现：API开发者完成API设计/开发/测试后，可以将API注册在华为云生态网关，然后在华为云云商店上架API商品并定价售卖，实现直接售卖API并获得商业收益。

版权所有 © 华为云计算技术有限公司

- 间接变现：API能力开放给应用开发者，供其在应用开发和集成中调用。应用生产出来后，可在华为云云商店上架SaaS等应用类型商品，实现API的间接变现，获得商业收益。

 版权所有 © 华为云计算技术有限公司

5 产品功能

表 5-1 API 中心功能概览

功能名称	功能描述	发布区域
API设计和测试	API开发者可使用API中心工具库中的API生产工具（如华为云API Arts），进行API的设计、测试等。	华北-北京四
服务商入驻	API开发者可在线申请入驻成为API中心的服务商。	华北-北京四
API资产管理	API中心服务商可在API中心管理控制台管理API资产。	华北-北京四
API网关代理	API中心服务商可使用API中心的网关代理模块，进行API注册、发布，并支持配置流控策略、访问控制、签名密钥等策略来限制对API的访问。	华北-北京四
API门户	API中心门户汇聚展示千行百业API，为应用开发者提供统一的API搜索查找入口，并通过智能搜索和推荐，帮助开发者快速找到所需API。	华北-北京四
在线调测	应用开发者可在API门户的API详情页进行API在线调测，快速试用API。 **说明** API是否支持调测，取决于伙伴服务商上架API资产时是否提供了相关试用调测环境。部分API暂未提供调测能力。具体功能以API详情页面展示的为准。	华北-北京四
API凭证获取	• 对于技术开放型API，应用开发者可根据API使用指南中的指定方式或者联系API服务商获取API调用凭证。 • 对于商业售卖型API，应用开发者可根据页面引导前往云商店通过购买获得API调用凭证。	华北-北京四

版权所有 © 华为云计算技术有限公司

6 计费说明

API中心当前是免费的平台服务，当前API中心平台本身并不直接面向伙伴/开发者收取费用。

API商业售卖是基于华为云云商店来实现交易和变现，该场景下计费相关信息以华为云云商店相关规定为准。

版权所有 © 华为云计算技术有限公司

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。

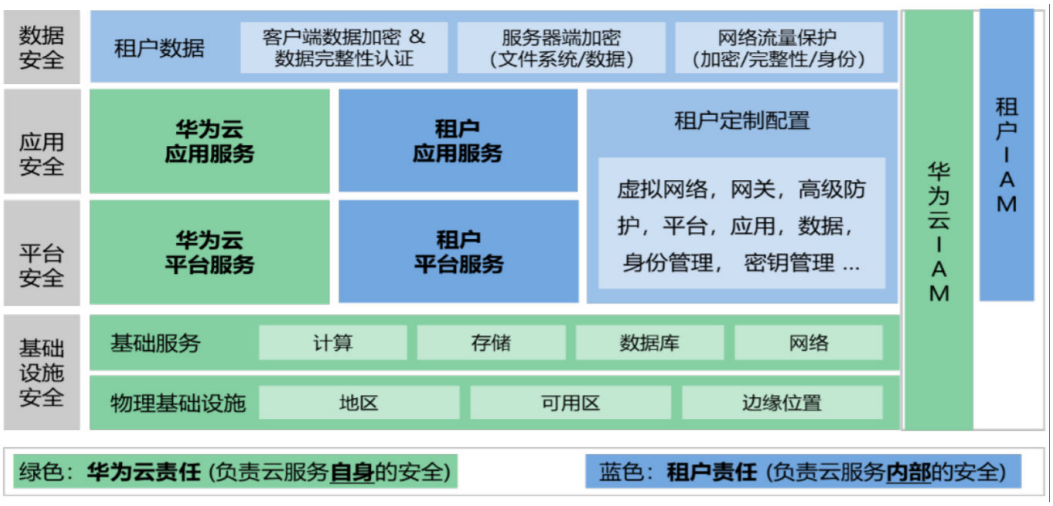
安全性是华为云与您的共同责任，如**图7-1**所示。

- 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各类各项云服务自身的安全，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类各项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。

版权所有 © 华为云计算技术有限公司

图 7-1 华为云安全责任共担模型



7.2 身份认证与访问控制

身份认证

- 服务认证：API网关代理提供AK/SK、Token等多种方式进行服务认证，只允许授权的访问。
- 签名密钥：API网关代理提供签名密钥，用于后端服务校验API网关代理是否合法。

访问控制

- 流量控制：API网关代理支持从用户、IP、凭据和时间段等不同的维度限制对API的调用次数，保护后端服务。
- 访问控制：API网关代理支持通过设置IP地址或账户的黑白名单来禁止/允许某个IP地址或账户访问API，保护后端服务。

7.3 服务韧性

API中心提供了4级可靠性架构，通过全局部件跨Region容灾、Region部件跨AZ容灾、AZ内集群容灾、数据库主备容灾，保障服务的持久性与可靠性。

表 7-1 API 中心可靠性架构

可靠性方案	简要说明
跨Region容灾	全局级部件支持跨Region容灾，当主Region异常后，全局业务可以切换到备Region继续运行。
双AZ容灾	Region级部件实现跨AZ双活，一个AZ异常时不影响云服务持续提供服务。
AZ内集群容灾	通过集群提供服务，集群中每个微服务都有多个实例，当一个或部分实例异常时，其他实例可以持续提供服务。

版权所有 © 华为云计算技术有限公司

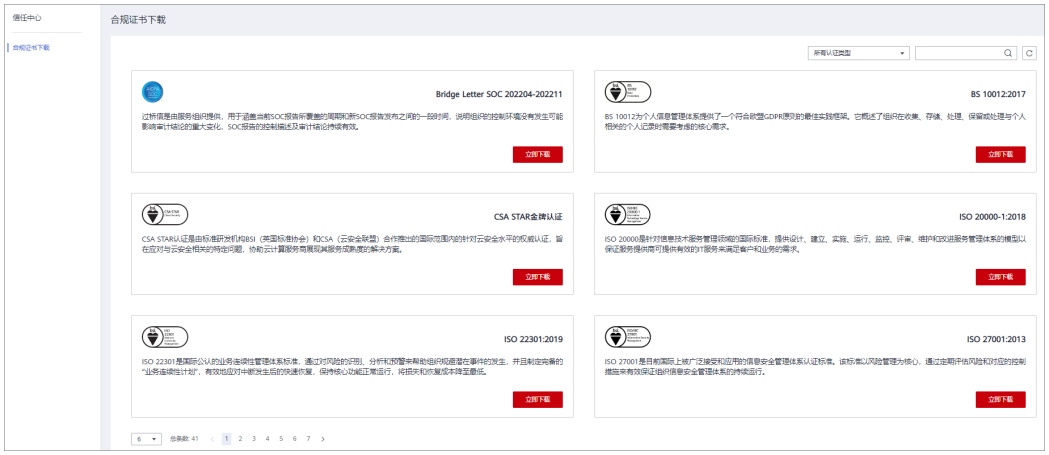
可靠性方案	简要说明
数据容灾	数据存储在RDS服务中，RDS实现了AZ容灾方案，数据持续会同步到容灾站点，当生产站点的RDS异常后，容灾站点可以接管业务，保障云服务持续运行。

7.4 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 7-2 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**。

版权所有 © 华为云计算技术有限公司

图 7-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 7-4 销售许可证&软件著作权证书

版权所有 © 华为云计算技术有限公司

8 约束与限制

API中心的使用限制如下：

- 创建API资产：每个用户最多可以创建50个API资产。
- API网关代理：API网关代理使用限制如表8-1所示。

表 8-1 API 网关代理使用限制

限制项	限制值
API分组数量	每个用户最多可以创建50个API分组。
独立域名数量	每个分组最多可以绑定5个独立域名。
API数量	每个用户最多可以创建200个API。
后端策略数量	每个API最多可以创建5个后端策略（不包含默认后端策略）。
凭据数量	每个用户最多可以创建50个凭据。
流量控制策略数量	每个用户最多可以创建15个流量控制策略。
签名密钥策略数量	每个用户最多可以创建5个签名密钥。
访问控制策略数量	每个用户最多可以创建5个访问控制策略。
环境数量	每个用户最多可以创建5个环境（包含默认的RELEASE环境）。
环境变量数量	每个分组在任意一个环境中，最多可以创建50个环境变量。
负载通道数量	每个用户最多可以创建10个VPC通道，每个负载通道最多可以添加10个服务器。
参数数量	每个API最多可以创建50个参数。

版权所有 © 华为云计算技术有限公司

限制项	限制值
发布历史数量	同一个API在每个环境中最多记录10条最新的发布历史。
每个API的访问频率	不大于200次/秒。
特殊应用	每个流控策略最多可以创建30个特殊应用。
特殊租户	每个流控策略最多可以创建30个特殊租户。
子域名访问次数	每个子域名每天最多可以访问1000次。
调用请求包的大小	API每次最大可以调用12M的请求包。
TLS协议	支持TLS1.1和TLS1.2，推荐使用TLS1.2。

说明

- 本章描述的“用户”指的都是华为云账号。
- 如果API网关代理当前的配额限制无法满足您的需求，您可以向系统提交工单申请更多配额。

版权所有 © 华为云计算技术有限公司

9 与其他服务的关系

API Arts

API中心将API Arts作为API生产工具提供给API开发者，并支持API开发者将工具中的API文档一键发布到API中心进行分享和开放。

API Explorer

API中心对接集成API Explorer，并将其作为API中心的API调试功能模块，支持开发者在API中心直接试用API。

华为云云商店

API中心聚集API开发者和应用开发者，并汇聚技术分享和商业售卖的所有API，为云商店引流；云商店提供商业变现通道。

华为云集成工作台

API中心可以通过对接aPaaS集成工作台的集成框架，支持aPaaS集成工作台获取并使用API资产元数据，用于连接器的创建和使用。

版权所有 © 华为云计算技术有限公司

10 基本概念

API

API（Application Programming Interface，应用程序编程接口）是一些预先定义的函数，应用将自身的服务能力封装成API，并通过API网关代理开放给用户调用。

API包括基本信息、前后端的请求路径、参数以及请求相关协议。

API 分组

API分组是同一种业务API的集合，API开发者以API分组为单位，管理分组内的所有API。

域名管理

在开放API前，您需要为API分组绑定独立域名，API调用者通过独立域名访问分组内的API。

环境

为了方便管理API的生命周期，API网关代理定义了API受限使用范围，这个受限使用的范围，称为环境。例如：API的测试环境，开发环境等。

环境定义了API生命周期管理过程中的不同状态，API可以被发布到不同的自定义环境中。

调用不同环境的API，一般通过在API调用的请求头增加指定的头部参数，头部参数名固定为x-stage，它的取值为环境名，用以区分不同的环境。

环境变量

在环境上创建可管理的一种变量，该变量固定在环境上。通过创建环境变量，实现同一个API在不同环境中调用不同的后端服务。

流量控制

流量控制支持从用户、凭据、源IP和时间段等不同的维度限制对API的调用次数，保护后端服务。

API网关代理支持按秒、分钟、小时、天粒度级别的流量控制。

版权所有 © 华为云计算技术有限公司

访问控制

访问控制策略是API网关代理提供的API安全防护组件之一，主要用来控制访问API的IP地址和账户，您可以通过设置IP地址或账户的黑白名单来禁止或允许某个IP地址或账户访问API。

凭据

凭据定义了一个API调用者的身份。API中心支持将一个API授权给多个凭据，也支持将多个API授权给同一个凭据。

签名密钥

签名密钥由一对Key和Secret组成，用于后端服务验证API网关代理的身份，在API网关代理请求后端服务时，保障后端服务的安全。

当签名密钥绑定API后，API网关代理向后端服务发送此API的请求时，会增加相应的签名信息，此时，后端服务依照同样方式进行签名并得到签名结果，如果签名结果和API网关代理传过来的Authorization头中的签名一致，则可证明API请求确实来自API网关代理，而不是其他伪造请求。

VPC 通道

API网关代理通过VPC通道访问部署在VPC内的服务，您可以借助API网关代理将部署在VPC中的后端服务开放给第三方用户调用。

简易认证

简易认证指调用API时，在HTTPS请求头部消息增加一个参数X-Apig-AppCode（参数值填AppCode），而不需要对请求内容签名，API网关代理也仅校验AppCode，不校验请求签名，从而实现快速响应。

版权所有 © 华为云计算技术有限公司

11 附录-API 治理规范指导

11.1 概述

11.1.1 简介

目的

主要用于指导伙伴、开发者在华为云API中心生产和开放API。通过统一的API治理框架和规范，帮助伙伴、开发者构建并提供有质量保障的API服务，为平台营造良好能力开放与交互的环境，支撑华为云和伙伴及开发者共建API生态。

API治理规范主要从安全、可用性、易用性、可维护性，生命周期管理六个维度针对API生产（API设计/开发/测试）和API开放提供规则建议。

- 安全：对API的安全认证、涉及敏感信息或个人隐私数据使用和处理提出规范要求或建议，保障API的安全合规。
- 可用性：对API调用成功率、响应时长、并发及流量控制、吞吐量等提出规范要求或建议，保障API的高可用性。
- 易用性：对API参考文档描述、入参和出参、消息头定义等提出规范要求或建议，提升API调用者使用体验。
- 可维护性：对于API兼容性、日志实时性和完整性、版本管理等提出规范要求或建议，提升API可维护性。
- 生命周期管理：对API变更和下线等提出规范要求或建议，保障已订阅API租户的业务连续性。

包含Must类型的基本规则以及Should类型的扩展规则。Must规则牵引API开发者提供符合企业级标准、安全合规的API，Should规则在提供更全面指导的基础上，给予开发者灵活的弹性空间，方便开发者更快的加入API生态圈。

适用范围

在华为云API中心发布、用于面向公众开放信息和服务的API。此类API可以充分发挥开发者的创造性，增加企业业务覆盖面和访问流量，是企业新的商业模式和收入来源。

版权所有 © 华为云计算技术有限公司

读者对象

API构建者包括：架构师、开发、测试、运维、产品经理、CTO等。

11.1.2 术语

API

API（Application Programming Interface，应用程序接口）是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

API Gateway

API Gateway（Application Programming Interface gateway，API网关）是当前API的一个公共服务，是所有API注册和发布的入口。

JSON

JSON(JavaScript Object Notation) 是一个轻量级的数据交换格式，它易于人类读写及其解析生成。

HTTP

HTTP（Hyper Text Transfer Protocol）是超文本传输协议。

HTTPS

HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer）是安全版超文本传输协议。

REST

REST（Representational State Transfer，表征状态转移）网络上的所有事物都可被抽象为资源，每一个资源都有唯一的资源标识（resource identifier），对资源的操作不会改变这些标识，所有的操作都是无状态的，使用标准方法操作资源。

RESTful风格的服务接口需定义：操作名、URL、请求和响应消息体和响应状态码。

本文后续章节将分别描述接口各部分的定义规范。

11.2 规范要求

11.2.1 API 生产

11.2.1.1 安全性

涉及敏感信息或个人隐私数据的 API，应提供数据传输和存储过程中的安全机制

本条规则是MUST类型的基本规则，可保障API的安全合规。

 版权所有 © 华为云计算技术有限公司

API接口参数传输和存储过程中，敏感信息和个人隐私数据禁止明文传输和存储，避免造成敏感信息或个人隐私数据泄露。敏感信息和个人隐私数据包括：

- 密码、AK/SK、Token等身份凭据。
- 密钥。
- 个人信息，如身份证号码、银行卡信息、家庭住址、健康信息等。
- 人与人之间的私人消息，如短信、电话通信内容。

API 涉及个人数据时，需要提供隐私声明

本条规则是MUST类型的基本规则，可保障API的安全合规。

如果API提供正常业务时涉及个人数据（包含收集、使用、转移、存储等），必须在API发布过程中提供产品隐私声明，描述收集的所有个人数据类型、目的、处理方式、时限等。

建议使用 POST/PUT 方式提交个人数据

本条规则是Should类型的扩展规则，给API开发者提供灵活的弹性空间。

在API设计过程中，使用POST/PUT请求来避免个人数据被缓存、记录。

说明

HTTP请求方法中，POST请求是向指定的资源提交要被处理的数据，其响应不会被缓存；PUT请求用来提交数据时，其响应是不能被缓存的。

11.2.1.2 可用性

API 请求 URI 中如果存在特殊字符，需要进行转义编码

本条规则是MUST类型的基本规则，可保障API的高可用性。

某些字符，由于有特殊含义或者系统保留，容易被Web应用防火墙或者安全访问控制产品所阻断，导致URI调用不生效，因此不建议在URI中使用，如果必须要用需要用转义编码替换。

说明

转义说明可参考：RFC 2396（Uniform Resource Identifiers (URI): Generic Syntax）。

API 响应状态码应使用规范的 HTTP 状态码

本条规则是MUST类型的基本规则，可保障API的高可用性。

API响应所使用的状态码应使用规范的HTTP状态码，状态码所表达的状态与API响应状态保持一致。

具体的HTTP状态码使用可参考RFC 7231（Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content），常用状态码如**表11-1**所示。

 版权所有 © 华为云计算技术有限公司

表 11-1 常用状态码

状态码	状态码表示	状态码详细信息
200	OK	执行成功，如：查询成功响应。
201	Created	创建成功，如：创建记录成功。
400	Bad Request	客户端请求语义有误，当前请求无法被服务器理解或请求参数有误。
401	Unauthorized	当前请求需要用户验证，需要用户提供Token进行认证。
403	Forbidden	禁止访问某些资源，如权限不足时无法查询对应的信息。
404	Not Found	无法找到对应资源，如资源不存在。
405	Method Not Allowed	HTTP方法不能被用于请求相应的资源如：HTTP方法要求POST方法，请求中使用了GET方法。
406	Not Acceptable	请求资源的内容特性无法满足请求头中的条件。
413	Payload Too Large	请求提交的实体数据大小超过了服务器够处理的范围。
414	URI Too Long	请求的URI长度超过了服务器能够解释的长度。
415	Unsupported Media Type	当前请求的方法和所请求的资源，请求中提交的实体并不是服务器中所支持的格式。
500	Internal Server Error	服务器遇到了一个未曾预料的状况，导致了它无法完成对请求的处理。通常是服务器内部产生了错误，导致处理失败。
502	Bad Gateway	代理服务器尝试执行请求时，从上游服务器接收到无效的响应。

API 请求设置媒体类型和编码格式，响应内容格式需与响应设置媒体类型和编码格式一致

本条规则是MUST类型的基本规则，可保障API的高可用性。

- 在API请求中对媒体类型和编码格式的正确定义有助于服务端对请求体进行格式校验，避免出现因请求消息体格式错误导致的执行异常。
- API响应内容格式需要与响应设置媒体类型和编码格式一致。在API响应中对媒体类型和编码格式的正确定义有助于服务端对请求体进行格式校验，避免出现因请求消息体格式错误导致的执行异常。
  - API的默认媒体类型为“Content-Type: application/json”和“charset=UTF-8”。
  - 当使用非application/json媒体类型时，建议根据情况选择合适的媒体格式，具体情况如**表11-2**所示。

 版权所有 © 华为云计算技术有限公司

表 11-2 常见的媒体类型

分类	场景	媒体类型
文件上传/下载类	文件上传下载类的接口，直接传递的是文件内容。 **须知** 不建议使用该API进行文件传输。	application/octet-stream
表单提交	主要用于界面表单提交，该方法目前已经不属于主流提交手段，建议使用JSON格式进行表单提交。	application/x-www-form-urlencoded
混合多部分类型	传递混合多部分内容类的接口，比如既有文本内容，表单内容，也有二进制文件的。	multipart/form-data
SOAP协议	调用以SOAP协议的WebService。	text/xml或application/xml
纯文本类型	仅传递纯文本内容。	text/plain

11.2.1.3 易用性

API 名称必须易于理解、见名知义

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

- API名称要简洁、易于理解、见名知义，建议按照“动词+名词”格式。
- 在生产环境的API不能包含“test、uat、sit、beta”等字样，API名称只支持中文、字母、数字以及“_”或者"-"，API名称长度建议不超过150字符。

例如：易于理解的API名称应为“查询虚拟机列表”/“ListServers”、“创建VPC网络”/“CreateVPC”

API 描述信息必须易于理解，表述准确

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

- API描述信息要易于理解，字面表述准确，能说明API的用途，场景及约束。
- API描述信息建议使用Markdown格式编写，便于生成对应API文档，API描述信息长度建议不超过2000字符。

例如：发布API用于查询虚拟机列表。良好的API描述应为“通过虚拟机名称、IP地址、虚拟机型号查询当前租户下的虚拟机列表，列表包括虚拟机名称，所属VPC、虚拟机IP、虚拟机型号、操作系统版本。”

API 文档按照模板进行写作

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

API对外开放时，API文档建议使用统一的模板，以便保持API参考文档的一致性，易于开发者理解。在API参考文档中必须包含如下内容：

版权所有 © 华为云计算技术有限公司

- API目录，包括本次提供API的列表信息。
- API名称及API功能介绍。
- API请求方法和URI。
- API请求参数说明，包括Header、Query参数，需要明确字段内容和取值范围。
- API请求Body内容，Body内容需要明确请求结构体内容及各个字段的取值范围。
- API响应状态码，状态码及对应的说明。
- API响应参数说明包括Header参数，需要明确字段内容和取值范围。
- API正常响应Body内容，正常响应Body内容需要明确响应结构体内容及各个字段的取值范围。
- API异常响应Body内容，异常响应Body中描述及说明。

API 请求尽量少使用自定义消息头

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

标准消息头及其取值格式按照参考标准，并尽量最小化添加自定义消息头。

所有消息头命名格式一致，自定义消息头命名规范：用连词符“-”分隔单词，采用大驼峰方式如X-APIG-TOKEN。

API 响应报文使用分页，避免超长列表数据返回

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

- 获取资源集合的API建议支持分页。当资源数量较多时服务的查询API需要支持分页，避免一次查询获取的资源数量过多。
- 不支持分页查询，则服务应该要设置一个显示条数的默认值，避免一次返回过多资源。默认返回数量需要在接口参考中对外说明，避免调用者以为查询出了全量信息。查询条件中可以设定查询数量(limit)，位移量(offset)。查询资源列表需要返回符合查询条件的资源总数(count)、查询数量(limit)、位移量(offset)。

举例：查询虚拟机从第10条开始，查询后100条。

请求

```
GET /ecs/v1/projects/xxxxx/servers?offset=10&limit=100
```

响应

```
{
"resources":[
  {
    "id":"xxx",
},
…
  {
    "id":"xxx",
  }],
 "offset":10,
 "limit":100,
 "count":1540
}
```

API 入参/出参设计必须考虑开发者易于使用

本条规则是Should类型的扩展规则，可提升API调用者的使用体验。

版权所有 © 华为云计算技术有限公司

API设计的输入参数开发者要易于获取，输出参数要让开发者易于理解。降低开发者使用API的使用成本，提升API使用体验。避免API的输入参数要通过多次前置条件API的查询获得。

11.2.1.4 可维护性

API 需要保持向后兼容性

本条规则是MUST类型的基本规则，可保障API的可维护性。

- 现网API版本一般保留3个版本或以下，如果超过3个版本会增加API本身的维护量，建议对旧版本API进行下线处理。
- 服务端API改动必须保证所有的服务消费者不被破坏。API是服务端和客户端的契约，不能单方面破坏契约。通过如下的方式来保证向后的兼容性：
  - 遵循兼容扩展标准。
  - 忽略请求/响应中的未知字段。
  - 只添加可选字段，不能添加必选字段。
  - 不能更改字段的含义。
  - 当资源URL发生变化的时候，支持重定向。
  - 服务端提供新版本API的同时，需要对老版本API提供支持。

例如：应用A更新API查询虚拟机列表，增加多个新的查询条件。在API发布之后，之前订阅该API的应用不能因为增加了新的查询条件而造成查询虚拟机列表失败。

API 请求 HTTP 动词使用标准化且满足幂等性

本条规则是Should类型的扩展规则，可提升API的可维护性。

HTTP方法的需要符合幂等性的约束，幂等性的约束是指一次和多次请求某一个资源应该具有同样的副作用，单个资源操作，资源的标准CRUD操作对应的HTTP动词如表11-3所示。

表 11-3 HTTP 动词

方法	描述	幂等性
POST	适用于新建资源场景，以及CRUD无法表达的操作场景（Non-CRUD）。	否
GET	用于获取资源的场景，必须具备安全性。	是
PUT	如果操作的URL为一个新资源，则创建该资源。如果URL为一个已存在的资源，则替换该资源，传入的消息体需包含被替换资源的完整信息。如果传递的信息不完整，在服务实现端需提供对应信息的默认值。	是
DELETE	用于删除资源的场景。	是
HEAD	返回资源的元信息比如：ETag和Last-Modified之类的信息。	是

版权所有 © 华为云计算技术有限公司

方法	描述	幂等性
PATCH	用于部分更新资源的场景，如果使用PUT操作所需输入的整体资源信息内容大小与PATCH操作无太大差异，优先使用PUT操作，不推荐使用PATCH操作。	是
OPTIONS	获取当前资源支持哪些方法的信息。	是

例如：使用正确的HTTP动词。

- “查询虚拟机列表”： GET /servers
- “创建VPC网络”： POST /vpc
- “删除虚拟机标签”： DELETE /server/tag
- “创建/更新数据库实例元数据”： PUT /instance/metadata

API 建议明确标识出版本号

本条规则是Should类型的扩展规则，可提升API的可维护性。

每个API建议带上版本号，保证API的版本显性化，容易被API调用者所识别。版本号建议放置在URI中，用于显性标识所请求的API版本。

服务所提供的API版本定义统一规范成“vX”，这里X是一个正整数如：v1，v2等，要在API版本文档中明确在接口中说明清楚哪个版本号是目前服务主推的版本，哪些版本是支持但已经不推荐的版本，方便API调用者通过该接口快速了解与跟进服务API的变化。如果无法在URI中进行API版本标识，则可在HTTP Header中进行API版本标识。

例如：应用A提供API查询虚拟机列表GET /servers，可在URI上进行版本标识，如GET /v1/servers，GET /v2/servers，同时提供相关的API文档说明不同版本之间的区别。

11.2.2 API 开放

11.2.2.1 安全性

API 使用合适的认证模式

本条规则是Should类型的扩展规则，可提升API的安全性。

根据具体业务场景，选择API调用的认证模式，具体说明如表11-4所示。

表 11-4 认证模式说明

认证模式	认证描述
AppKey	在API请求Header或者Query中携带AppId和AppKey用于进行身份认证，该认证方法直接传递密钥，在使用过程中需要使用HTTPS协议保证传输安全。

版权所有 © 华为云计算技术有限公司

认证模式	认证描述
签名认证	请求Header或者Query中携带请求签名、请求时间和应用身份进行身份认证，该认证方法对请求中URI、HTTP方法、AppId、SignKey、请求时间等采用HMAC-SHA256进行计算，在API请求过程中不会直接传递SignKey，同时对请求时间进行有效校验，避免重复请求攻击。
动态Token	API请求可使用AppId及AppKey向Token服务器换取动态Token，在动态Token有效期内，在API请求Header中携带Token进行身份认证，由于在换取Token过程中传递AppKey，因此换取Token需要使用HTTPS协议保证传输安全。

11.2.2.2 可用性

API 需要配置并发请求及流量控制

本条规则是Should类型的扩展规则，可提升API的可用性。

在API发布之前，需要根据设计的服务等级标准进行流量控制设置。API流量控制包括三个部分：并发请求控制，吞吐量控制和传输流量控制。

- 并发请求控制：指API最大允许的客户端连接数量。
- 吞吐量（TPS）控制：指API单位时间内可并发处理的能力。
- 传输流量控制：指API单位时间内传输的数据量。

API 发布过程中必须保证 API 注册信息的准确性

本条规则是MUST类型的基本规则，可保障API的高可用性。

API发布是API生命周期中重要的部分，因此在发布过程中需要保证API的正确性、可读性、可用性，并对服务质量进行约束。

必须对API进行统一注册和统一管理，API注册目标系统为API中心。在API发布过程中必须保证API注册信息的准确性，保证API符合国家法规以及安全规定的要求。

API 调用成功率>=99.99%

本条规则是MUST类型的基本规则，可保障API的高可用性。

API调用成功定义：调用API时响应码为除5XX外其余响应码。API调用成功的次数/总的API调用次数*100%就是调用成功率，该数值应大于等于99.99%。

服务API实际可用性与承诺的服务可用性需要100%吻合。当发现无法达到承诺的服务可用性时，API提供方从架构上考虑，通过增加可用区，增加多活部署等手段提升服务API的整体可用性。

API 的 TP99 响应时长<3s

本条规则是MUST类型的基本规则，可保障API的高可用性。

要求从API网关到后端服务的API调用，99%的调用响应时长<3s，TP99响应时长就是满足百分之九十九的网络请求所需要的最低耗时。

版权所有 © 华为云计算技术有限公司

TP99响应时长达标率=TP99响应时间符合要求的API数量/总的API数量*100%，该数值应小于3s。

服务API实际响应时间应与承诺的服务响应时间比不应小于99%，即至少99%的API响应时间应达到承诺的服务响应时间。当发现无法达到承诺的服务响应时间时，API提供方应从架构上通过扩容、缓存等手段提升API响应时间。

禁止在 API 请求中携带超长报文体

本条规则是MUST类型的基本规则，可保障API的高可用性。

API通道默认请求报文体长度（Body Size）限制为2MB，默认请求Header长度（Header Size）限制为1MB。

明确 API 吞吐量与并发量

本条规则是Should类型的扩展规则，可提升API的可用性。

在API的设计阶段需要对单位时间可处理的能力进行设计，指标包括吞吐量和并发量。

- 吞吐量（TPS）是指服务在单位时间内处理请求的数量，使用单位时间为秒。
- 并发量是指服务可以同时承载的正常使用系统功能的用户的数量。

服务API的最大吞吐量/并发量与承诺的服务吞吐量/并发量需要100%吻合。当发现无法达到承诺的吞吐量/并发量时，API提供方应从架构上通过扩容等手段提升吞吐量和并发量。

11.2.2.3 可维护性

保证 API 日志采集的实时性及完整性

本条规则是MUST类型的基本规则，可保障API的可维护性。

在采集API调用日志过程中，需要保证API日志的实时性和完整性，以提升API分析的精准度。

- API日志在传递过程中，必须保证传递日志不会出现丢失。API日志总体丢失率小于0.5%。
- 在对API日志处理过程中，仅能对API日志进行增维操作，禁止对API日志中重要部分，如请求时间、请求者身份、请求IP地址、请求域名、请求URL地址、响应时间、响应状态码进行篡改。

11.2.2.4 生命周期管理

API 接口变更在参考文档中为新版本提供迁移计划

本条规则是Should类型的扩展规则，可方便管理API的生命周期。

在进行新版本API设计时应当考虑老版本升级迁移计划，从而实现API的迁移。新版本中继承的接口在语义上应当能兼容老版本。

- 对于计划不再支持的接口，需要正式发布接口变更公告，应当至少提前6个月在文档标识（使用@deprecated）为不建议使用（在此期间该接口仍要能完成正常的功能），并提供替换方式的处理。

版权所有 © 华为云计算技术有限公司

- 新版本API为兼容旧版本，增加的字段不建议作为强制填写的字段，字段取值范围不建议小于原有的取值范围。

API 文档记录 API 接口变更

本条规则是Should类型的扩展规则，可方便管理API的生命周期。

API接口的变更，要具体到参数级别，必须将API修订的记录按照时间和版本顺序排列进行条目化，具体示例如**表11-5**所示。

表 11-5 API 修订记录

时间	版本	变更内容
2021-07-15	V1.0	XXX服务API初始发布
2021-09-20	V1.1	1. XXX的API，增加XXX字段，用于XXXX功能；增加XXX字段，用于XXX功能。 2. XXX的API，增加XXX字段，用于XXX功能。

API 下线前必须提前通知订阅服务的用户

本条规则是MUST类型的基本规则，可保障API租户的业务连续性。

对于需要下线的API，需要梳理订阅该API的用户，并通过公告等方式向订阅API的用户进行提醒。通知需要在服务下线前至少6个月启动，并在公告服务下线时间后1个月内对API调用进行监控，当没有API调用流量之后，才启动正式下线。待该API到了正式下线后，API中心不再展示下线的API。

11.3 工具平台

API 生产阶段

API中心通过对接集成，为API开发者提供API Arts等自动化的API设计/开发/测试工具，开发者通过华为云账号登录后即可使用。

API 开放阶段

- API开发者（API提供方）可以在API中心**申请入驻为服务商**，然后自助发布上架API。上架成功后，API将在API中心的API门户面向开发者公开或指定范围内开放。API门户支持开发者（API使用方）在免登录情况下浏览、搜索API，通过华为云账号登录后，还可进行在线调测、购买或申请凭证等。
- API提供方可在API中心完成API发布、变更、下线等生命周期管理。

操作指导

相关操作指导，请参考华为云帮助中心**API Hub**。

版权所有 © 华为云计算技术有限公司

12 修订记录

发布日期	修订记录
2023-09-27	第八次正式发布。 新增如下章节： • **附录-API治理规范指导**
2023-07-14	第七次正式发布。 优化如下章节： • **约束与限制**
2023-05-22	第六次正式发布。 新增如下章节： • **图解API中心** 优化如下章节： • **产品优势**
2023-03-31	第五次正式发布。 优化如下章节： • **什么是API中心** • **应用场景** • **产品功能** • **与其他服务的关系**
2023-03-22	第四次正式发布。 优化如下章节： • **产品功能**
2023-03-03	第三次正式发布。 优化如下章节： • **产品功能**

版权所有 © 华为云计算技术有限公司

发布日期	修订记录
2023-02-10	第二次正式发布。 优化如下章节： ● 约束与限制
2022-12-14	第一次正式发布。

版权所有 © 华为云计算技术有限公司