

资源编排服务

产品介绍

文档版本 01
发布日期 2025-02-10



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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

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 基本概念	1
2 什么是资源编排	2
3 产品优势	3
4 应用场景	4
5 约束与限制	7
6 支持 Provider 版本列表	9
7 安全	11
7.1 责任共担	11
7.2 身份认证与访问控制	12
7.3 审计与日志	12
7.4 认证证书	13

1 基本概念

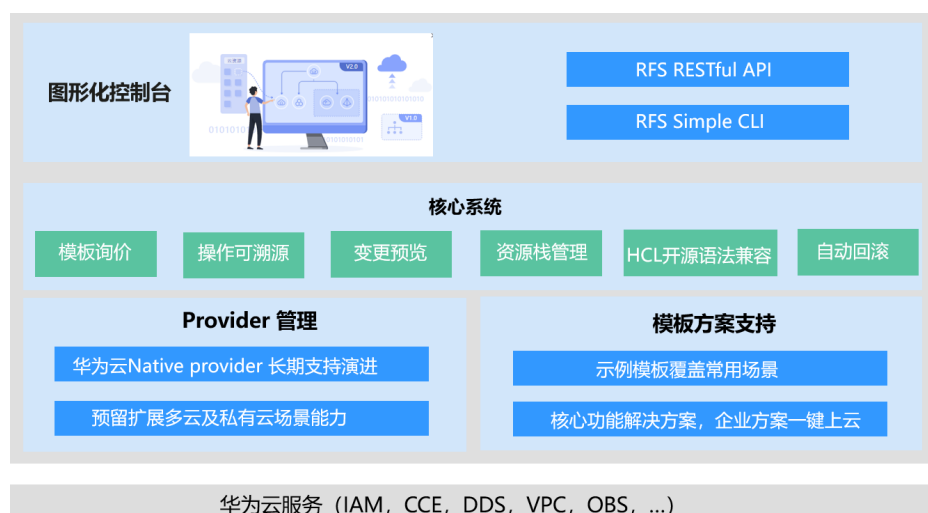
概念名称	描述
资源	一个云服务可以有多种资源。资源可以是VPC，虚拟机，也可以是某种微服务应用，或者是类似于安全策略，DNS记录等高层数据模型。
模板	模板是一个HCL语法文本描述文件，支持tf、tf.json、zip包文件格式，用于描述您的云资源。资源编排根据模板完成各种云资源的创建。
资源栈	资源栈是云服务资源的集合。资源栈将模板描述的所有云服务资源作为一个整体来进行创建、删除、更新、查询等。
执行计划	执行计划提供对资源栈变化的预览。这个执行计划展示了当前模板与线上资源的对比变化，清晰地展示了资源编排对资源与属性将要执行的操作（如新增、修改、删除等）。用户可以预览这个计划，在确认符合预期后，再执行这个计划。资源编排就会完成模板定义资源的创建、变更等。
资源栈集	统一管理多账号、多region下资源的堆栈集合的实体。通过部署堆栈集，可以部署其管理的所有堆栈从而管理多个堆栈下的资源。堆栈集是对堆栈管理功能的拓展。

2 什么是资源编排

资源编排是完全支持业界事实标准Terraform（HCL + Provider）的终态编排引擎，用于管理系统资源及服务资源（一切可定位、描述的物理或者逻辑实体，例如数据库，VPC，流水线，IAM中的Role）。资源编排采用业界开放生态HCL语法的模板，它按照模板自动化部署指定的云服务资源。

资源编排聚焦于华为云所用资源的自动化批量构建，帮助用户用高效、安全以及一致的方式新建、管理和升级所需资源，提升资源管理效率，降低资源管理变更带来的安全风险。

产品架构



3 产品优势

声明性：用户仅需直观描述所需资源的最终状态，屏蔽复杂的申请过程，降低资源管理的复杂度。

幂等：资源描述代码多次调用效果幂等，可确保不重复申请资源。

安全可靠：可视化的审计、安全、和合规控制策略，杜绝资源变更操作带来的安全风险。

生态丰富：南向生态支持华为云主流服务（90+云服务、540+资源对象，详情参见：[资源支持清单](#)），开箱即用；北向完全兼容HCL语法，无学习成本。

简单易用：向导式操作配合完善的资料、样例辅助体系，五步即可完成资源管理操作。

服务全托管全云化：用户不需要安装任何软件、不需要准备执行机、不需要管理底层文件和数据就可以完成资源的自动化管理。

自动回滚：资源部署失败自动将所有资源状态返回上一个成功部署的状态。

4 应用场景

应用上云

场景描述

应用上云时，很多工作需要手工重复操作，例如环境的销毁和重建、在扩容的场景下重复完成多个新实例的配置等，手工操作容易带来操作失误。

同时应用上云时，很多操作非常耗时，例如创建数据库、创建虚拟机等，手动操作容易失误，串行创建多个任务，就需要您持续等待较长时间。

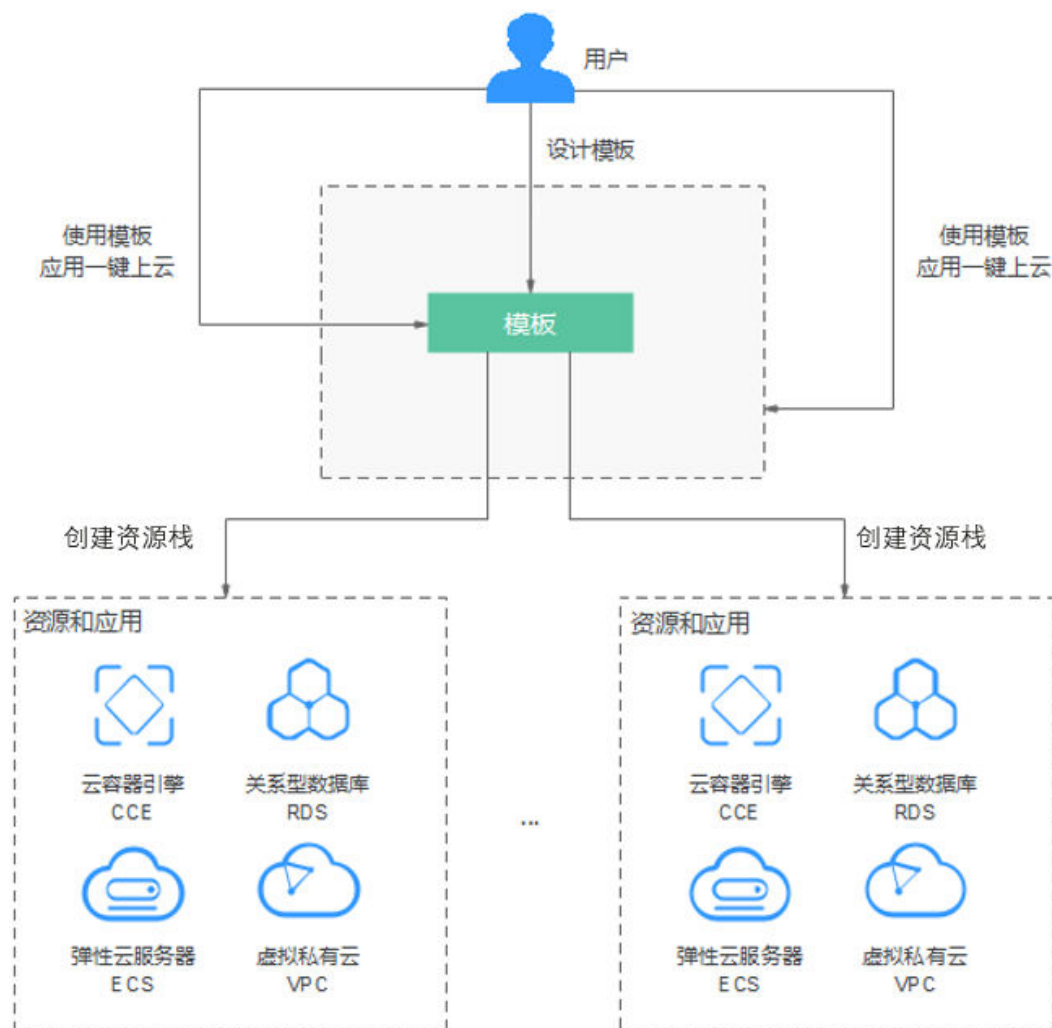
解决方案

资源编排就是将上述场景的工作进行工具化、流程化。资源编排采用模板对应用所需资源进行统一描述；资源栈管理功能提供众多资源自动化部署或销毁操作。资源编排可以将大批量、不同服务、不同规格的资源实例，统一定义在模板中。完成自动化创建，实现资源的快速部署和灵活配置。

收益优势

- **简单易用**
通过编写模板，即可完成应用设计与资源的规划，使业务的组织和管理变得轻松。
- **高效执行**
向导式自动完成部署或销毁操作，省去繁琐的人工操作，减少了人为操作的失误。
- **快速复制**
同一模板可以多次重复使用，自动化构建相同的应用与资源到不同的数据中心。提升了您的工作效率。

图 4-1 应用上云场景



ISV 资源发放

场景描述

独立软件开发商(ISV)需要快速将软件所需资源部署到云上，供其众多的客户进行使用。传统的软件发放的方式是在其官网提供软件的代码下载及平台搭建指南。但该方式需要ISV自行组网、交付资源、部署软件，准备时间长，成本高。

解决方案

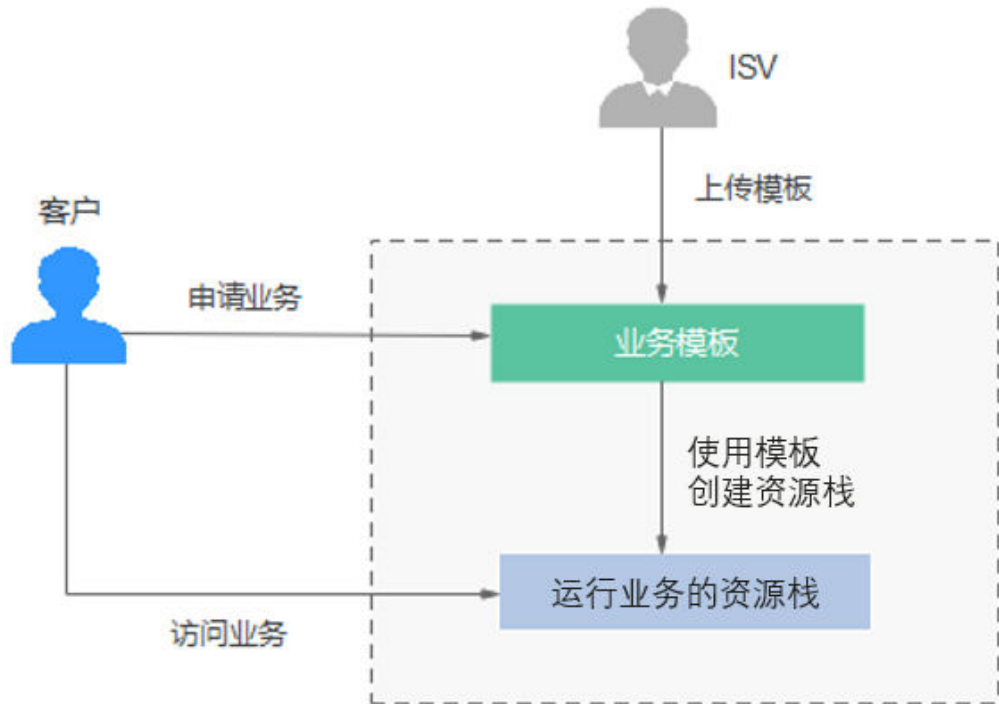
资源编排提供了标准化的资源和应用交付方式。ISV可以通过将软件服务模板化。通过资源编排的资源栈部署能力，对自身客户进行快速业务发放，将交付过程流程化。资源编排使用代码形式模板描述整个交付环境，也便于ISV将交付与CI/CD流程集成。

收益优势：

- 交付标准化**
 通过模板、资源栈方式将软件交付过程标准化，便于总结成最佳实践以便推广。
- 提升效率**
 通过模板，自动化完成资源的开通，ISV只需部署资源栈，即可完成业务的交付；提升了ISV的交付效率。

- **准确创建**
ISV的软件本身及所需的云服务资源都通过模板固化，减少人工失误带来的影响。
- **CI/CD集成**
可以将资源编排集成到现有工具链中，提升自动化程度。

图 4-2 ISV 资源发放场景



5 约束与限制

权限

资源编排需要[创建委托权限](#)。

配额

资源编排对单个用户资源栈数量限定了配额，如下表所示。

如果您需要添加更多的模板或创建更多的资源栈，请[提交工单](#)申请。配额的详细信息请参见[关于配额](#)。

资源类型	限制项	限制值
模板	每个华为云账号允许创建的最大模板个数	100
	模板名最大长度	128字符
	模板文件名称	255字节（一个中文字符=3个字节）
	模板URL地址长度	2048字节
	创建模板或版本接口参数 template_uri 传递文件内容最大值	解压后1M
	创建模板或版本接口参数 template_body 传递文件内容最大值	50 KB
资源栈	每个华为云账号允许创建的最大资源栈个数	100
	资源栈创建超时时间	6h
	资源栈名称长度	128字符

资源类型	限制项	限制值
执行计划	执行计划命名最大长度	255b
	每个资源栈中允许创建的最大执行计划数量	100
资源栈集	每个华为云账号允许创建的最大资源栈集个数	100
	每个资源栈集中允许创建的最大资源栈实例数量	100
	单个资源栈集操作最长运行时间	6h

6 支持 Provider 版本列表

Provider是将各类资源的API（比如资源的CRUD操作API）封装而成的插件，供资源编排引擎调用。

资源编排支持Provider类型与版本如下表。

类型	介绍	版本	支持云服务数	支持资源数
terraform-provider-huaweicloud	用户可以用华为云的provider与华为云上的各种资源进行交互。provider在使用前，需要配置相应的权限。	1.72.1	96	846
		1.71.1	96	800
		1.70.2	97	746
		1.70.1	97	746
		1.69.1	97	730
		1.68.1	96	687
		1.67.1	96	664
		1.66.3	96	641
		1.66.2	96	637
		1.66.0	96	634
		1.64.4	95	603
		1.61.1	94	525
		1.59.1	92	474
		1.58.0	92	461
		1.57.0	91	426
1.56.0	91	413		
1.54.1	88	388		
1.52.0	87	367		

类型	介绍	版本	支持云服务数	支持资源数
		1.50.0	86	350
		1.49.0	83	346
		1.48.0	82	324
		1.47.1	82	296
		1.46.0	83	282
		1.44.1	80	270
		1.43.0	71	252
		1.42.0	68	236
		1.41.0	63	225
		1.40.2	63	225
		1.40.1	63	225
		1.40.0	63	225
		1.39.0	63	221
		1.38.2	33	117
		1.38.1	33	117

7 安全

7.1 责任共担

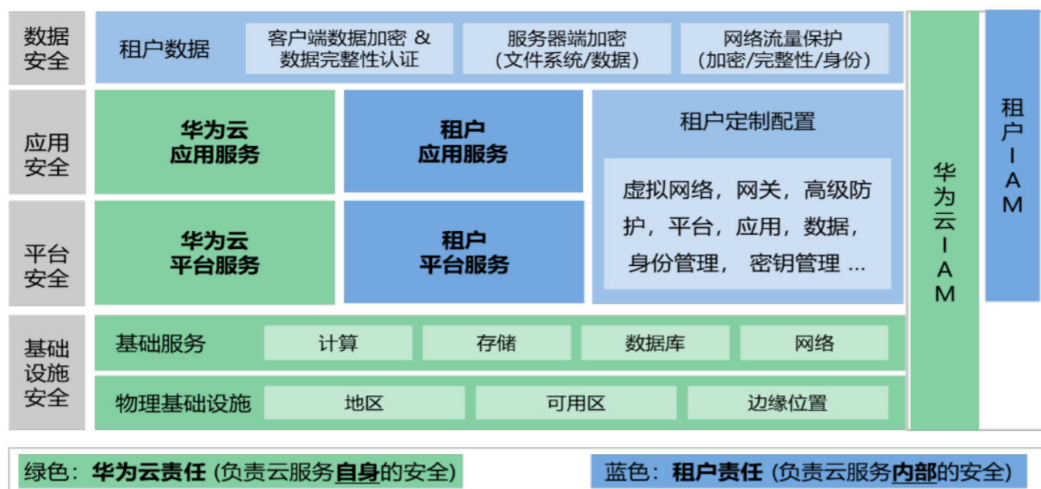
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

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。

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

租户使用RFS服务通常有两种调用方式：控制台访问和API调用。

1.控制台身份认证方式

RFS对接了统一身份认证服务（Identity and Access Management, IAM）。RFS租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management, 简称IAM）是华为云提供权限管理的基础服务，可以帮助RFS服务安全地控制访问权限。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对RFS资源的访问范围。IAM权限可以通过细粒度定义允许和拒绝的访问操作，以此实现RFS资源的权限访问控制。

2.API调用身份认证方式

所有的API接口调用均需要经过认证的请求才可以访问成功，经过认证的请求需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子，结合请求体携带的特定信息计算而成。通过访问密钥（AK/SK）认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。关于访问密钥的详细介绍及获取方式，请参见[如何获取AK/SK？（账号）](#)。

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。

RFS支持审计的操作事件，请参见[云审计服务支持的RFS操作列表](#)。

日志

用户开通云审计服务并创建和配置追踪器后，CTS可记录与RFS相关的操作事件，方便您进行事后审计。您可以在CTS控制台，事件列表菜单中，搜索RFS的事件来源，即可查看所有RFS相关的审计日志。

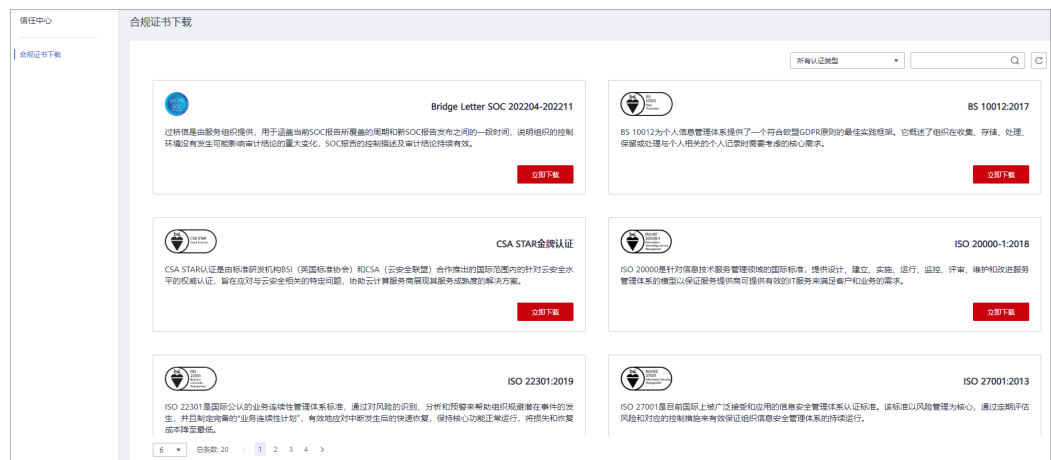
审计日志查看方法，请参见[查看云审计日志](#)。

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](#)。

图 7-3 资源中心



