制品仓库

产品介绍

文档版本 02

发布日期 2023-07-04

华为技术有限公司

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。

安全声明

漏洞声明

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该政策可参考华为公司官方网站的网址：https://www.huawei.com/cn/psirt/vul-response-process。
如企业客户须获取漏洞信息，请访问：https://securitybulletin.huawei.com/enterprise/cn/security-advisory。

目 录

1 图解制品仓库

2 什么是制品仓库

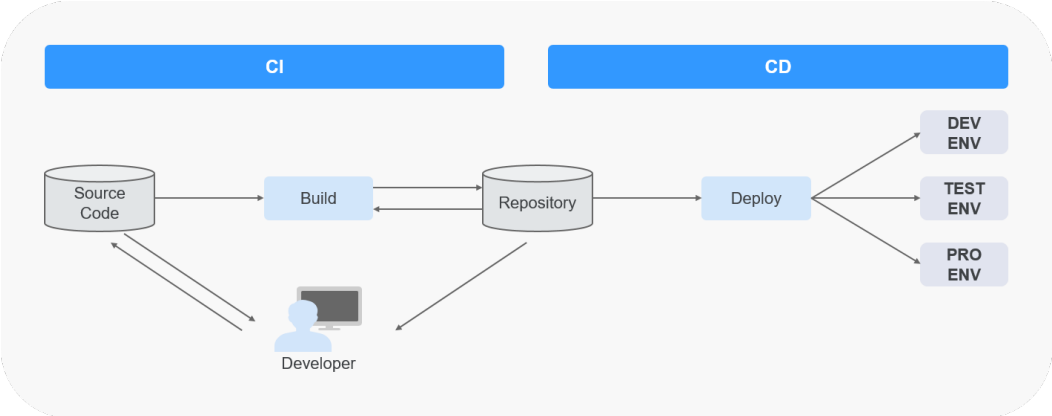
服务概述

制品仓库服务（CodeArts Artifact）为软件开发企业提供管理软件发布过程的能力，保障软件发布过程的规范化、可视化及可追溯。

相对于开发过程中的“源代码”，制品仓库服务关注和管理的是开发产生的待部署的“软件包”（通常由源码编译构建或打包而成）及其生命周期元数据（如名称、大小等基本属性、代码库地址、代码分支信息、构建任务、构建者、构建时间）。

“软件包”及其属性的管理是发布过程管理的基础，也是软件开发过程中的重要资产，常见的软件研发过程如图2-1所示：

图 2-1 软件开发过程



图中的Repository即制品仓库，用于管理软件开发过程产生的软件包，它是连接持续集成和持续交付的重要环节，软件包的发布评审、追溯和安全控制等操作通常在其中进行。

制品仓库服务提供以下两类仓库：

- 软件发布库。

  软件发布库可以存储任何软件包和工具，没有格式限制。

  通过编译构建任务可将产物归档到软件发布库，通过页面可以查看和管理这些归档的软件包及其生命周期属性信息，部署服务使用的部署软件包也来源于此。

- 私有依赖库。

  私有依赖库管理各种开发语言对应的私有组件包（开发者通俗称之为私服，如Maven私服），

  因为不同的开发语言组件通常有不同的归档格式要求（例如Maven组件需要基于GAV格式归档），该仓库目的就在于管理私有开发语言组件并在企业或团队内共享给其他开发者开发使用。

制品仓库服务提供哪些功能?

表 2-1 软件发布库功能特性

功能特性	说明
页面上传、下载、搜索、删除软件包，创建文件夹。	通过软件发布库页面进行类似网盘的操作来管理软件包。
查看软件包属性。	在软件发布库中可以查看软件包的生命周期属性，如基本信息（名称、大小、校验和等）、构建信息（构建任务、构建时间，源码仓库等）。
编译构建发布软件包到软件发布库。	软件发布库默认集成了编译构建服务，编译构建服务生产的所有软件包都可以通过配置自动上传到软件发布库中归档。
集成部署服务。	软件发布库中存储的软件包可以供部署服务使用。
包视图和构建视图。	可以根据需要选择从包视图（存储目录结构）或者构建视图（构建任务及流水线）的角度查看软件包。

表 2-2 私有依赖库功能特性

功能特性	说明
页面上传、下载、删除、搜索组件。	通过私有依赖库页面进行类似网盘的操作来管理私有组件。
编译构建发布组件到私有依赖库。	用户可以在编译构建任务中配置将构建产物直接发布到私有依赖库。
对接本地开发环境。	通过页面给出的使用配置，可以一键生成配置文件。将生成的文件配置到本地开发工具中以后，可以直接在本地开发环境对接私有依赖库中的私有组件包，例如使用命令行对私有依赖库中的组件进行上传、下载等操作。
仓库权限控制。	管理员可以通过设置成员在各仓库的角色来限制其在私有依赖库的操作权限。
对接容器镜像服务。	Docker私有依赖库引用容器镜像服务，用户可以查看和管理Docker私有镜像、新建和管理归档Docker私有镜像的组织。

3 产品优势

华为云CodeArts Artifact服务丰富了常用语言的制品库管理，实现制品开源合规扫描、制品生命周期管理、高效查看和搜索、自定义代理仓库和聚合仓，持续为客户提供全面、高效、可信的制品管理。

提供自研、安全、极致性能的制品仓，保障业务连续性不中断

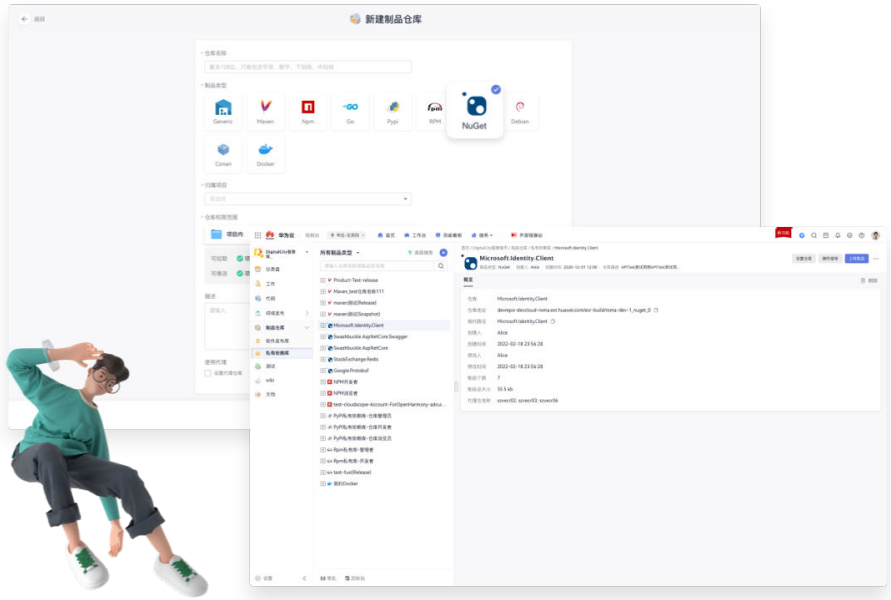
CodeArts Artifact制品仓库，基于云原生架构自研，解决外界不可控因素导致业务连续性问题。在安全上华为云CodeArts Artifact提供多维度、细粒度的权限控制，支持企业内不同角色对制品仓库访问控制的诉求。制品仓库存储采用物理隔离存储方式，减少恶意盗取制品风险，同时提供记录用户操作功能，保证操作可追溯；在可靠性上华为云CodeArts Artifact支持双AZ容灾和跨地域容灾、API限流与降级、服务依赖和隔离、实现服务故障自探测，实现99.99%的SLA保证；在极致性能上CodeArts Artifact提供热点文件缓存加速，增量上传下载，大小文件充分利用缓存加速优势，极速传输，提升用户构建速度，突破底层存储带宽限制，实现同地域高速并发传输，对比开源同类产品5X倍的上传和10X倍的下载性能提升。

支持开源合规分析和漏洞检测，让高危致命问题无处遁逃

华为云CodeArts Artifact制品仓库提供基于软件包的成分分析能力，通过特征匹配的方式，分析软件包中的开源软件及版本，并通过漏洞库匹配的方式进行开源漏洞排查。实时同步NVD、CNVD、CNNVD等常见漏洞库漏洞数据，覆盖主流编程语言(C/C++、Java、Go、Python、JavaScript等)，覆盖语种持续增加，提供全面、直观的风险汇总信息。在服务上线之前能够实时感知开源高危风险，建立起防御体系，并且及时修复问题，避免不可估量的损失。

支持 10+种仓库类型，充分满足用户各种使用场景

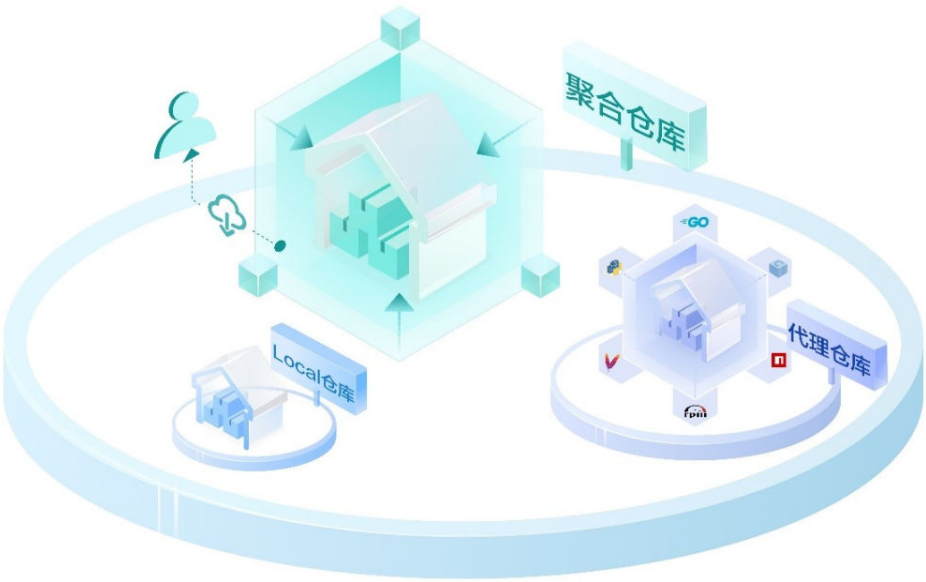
华为云CodeArts Artifact制品仓库支持Generic、Maven、npm、Go、PyPI、RPM、Debian、Conan、Nuget等10+种主流制品仓库类型，满足嵌入式、WEB应用、移动应用等开发场景所需，可以与本地各构建、部署工具和云上的持续集成、持续部署无缝结合。华为云CodeArts Artifact也提供制品和元数据的完整性校验能力，支持细粒度控制和按版本的细粒度包锁定权限，保障发布软件测试完整性，全面看护企业制品安全。



无缝连接第三方仓库，提供统一聚合仓地址，极大提升用户体验和下载性能

针对用户同时使用多个镜像源或制品库的场景，CodeArts Artifact提供仓库聚合能力，允许灵活组合多个代理仓，提供统一制品仓库入口，解决用户找不到制品包的痛点和简化客户配置。

CodeArts Artifact新增自定义代理仓功能，允许用户创建自定义代理仓库来代理开源社区仓库和三方依赖仓库，通过代理仓下载文件后支持将对应文件缓存到制品仓库，解决用户三方依赖下载慢痛点，实现下载三方依赖和本地仓库一样的极致体验。



按文件名和 checksum 搜索，亿级制品包秒级查询与精准定位

华为云CodeArts Artifact具备强大的搜索能力，依托于数据引擎检索能力，支持内部研发近百亿制品文件的多维度的快速搜索。

当前覆盖Maven、Npm、Go、PyPI、RPM、Debian、Conan、Nuget多种制品类型，用户可以通过文件名称或HASH信息（MD5、SHA1、SHA256、SHA512等四种类型）,实现秒级检索定位。 以此为基础，CodeArts Artifact也演进出上亿级别的元数据和SBOM的高效关联查询，以便对制品文件进行快速溯源，对比开源同类产品搜索性能提升20X倍。

4 安全

4.1 责任共担

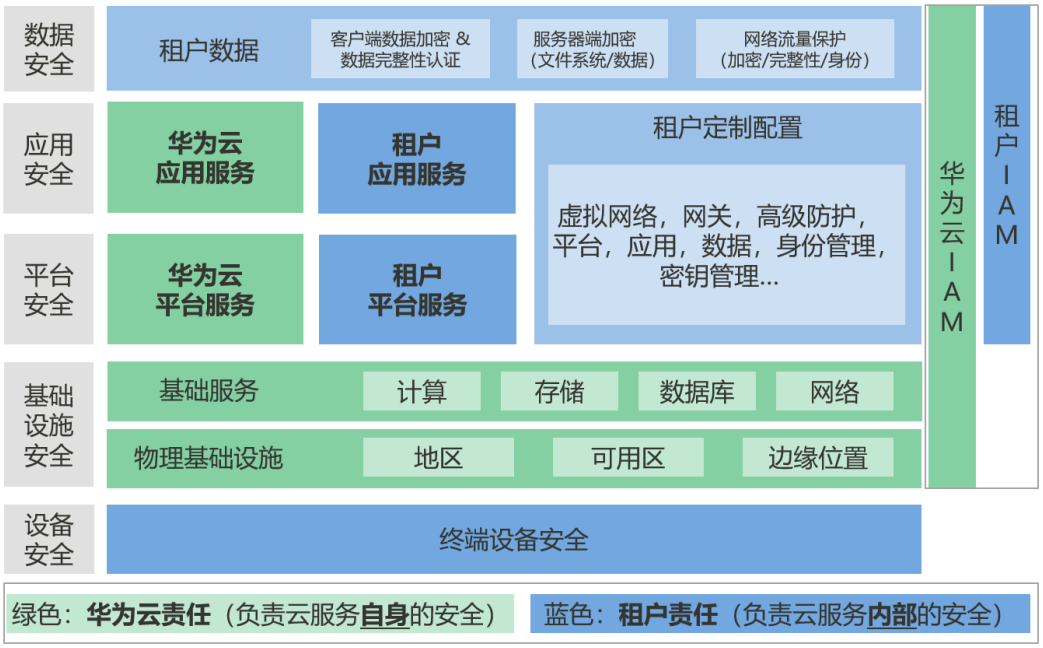
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图4-1**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，以及身份帐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 4-1 华为云安全责任共担模型



4.2 身份认证和权限管理

身份认证

用户通过管理控制台或API接口方式访问CodeArts Artifact服务，本质上都是调用API接口。

调用接口前，需要先通过统一身份认证服务（Identity and Access Management，简称IAM）的权限认证并获取对应Token，才能成功访问接口。

权限管理

CodeArts Artifact包含两个部分，软件发布库和私有依赖库。

- 软件发布库权限管理：软件发布库的权限可以实现项目下各角色权限分配自定义，具体操作请参考**权限设置**。
- 私有依赖库权限管理：私有库的权限由用户角色和仓库角色共同决定，用户角色本质为IAM权限，IAM权限获取需要管理员创建IAM用户后，将其加入用户组，并给用户组授予策略或角色，用户组中的用户也相应的获得对应的权限；仓库角色可以由拥有tenant administrator用户角色的用户进行分配，详细操作请参见**管理私有依赖库**中的管理用户权限章节，更细粒度权限管理请参见**管理私有依赖库**中的管理用户权限章节后的权限列表。

4.3 数据保护技术

CodeArts Artifact通过多种数据保护手段和特性，保证通过CodeArts Artifact的数据安全可靠。

数据保护手段	简要说明
传输加密（HTTPS）	CodeArts Artifact使用HTTPS传输协议，保证数据传输的安全性。
个人数据保护	CodeArts Artifact通过记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。
隐私数据保护	涉及到用户的仓库密码信息需要存储时，CodeArts Artifact提供敏感数据加密存储。

4.4 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CodeArts Artifact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**。

4.5 服务韧性

CodeArts Artifact通过多活无状态的跨AZ部署、AZ之间数据容灾等技术方案，保证业务进程故障时快速启动并修复，以保障服务的持久性和可靠性。

4.6 更新管理

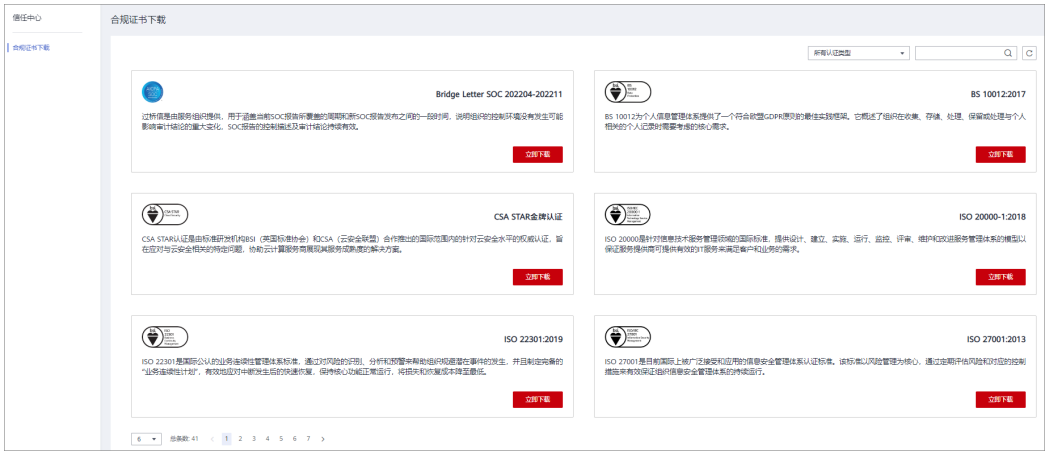
CodeArts Artifact对接凭证托管服务CCMS服务管理服务凭证，保证明文的有效凭据不落盘，并保持定期轮转。

4.7 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 4-2 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 4-3 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**。

5 约束与限制

介绍制品仓库服务中的使用限制，如表5-1所示。

表 5-1 制品仓库使用限制说明

指标类别	指标项	限制说明
浏览器	类型	目前制品仓库服务适配的主流浏览器类型包括： • Chrome浏览器：支持和测试最新的3个稳定版本 • Firefox浏览器：支持和测试最新的3个稳定版本 • Microsoft Edge浏览器：Win10默认浏览器，支持和测试最新的3个稳定版本 • IE浏览器：不再进行支持与测试。 **推荐**使用**Chrome**、**Firefox**浏览器，效果会更好。
分辨率	分辨率大小	推荐使用1280*1024以上。
软件发布库使用限制	通过页面上传单文件大小限制	2GB
	通过编译构建任务上传单文件大小限制	5GB
私有依赖库使用限制	总存储容量	1TB
	通过页面上传单文件大小限制	Maven/npm/PyPI/Go/RPM/Debian：100MB NuGet：20MB **说明** 私有依赖库单文件上传限制适用于非Docker格式仓库，Docker格式仓库的上传限制遵循SWR配额。

指标类别	指标项	限制说明
	通过编译构建任务上传单文件大小限制	300MB