开源治理服务

产品介绍

文档版本 01

发布日期 2025-06-30

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 什么是开源治理服务

开源治理服务（CodeArts Governance）是针对软件研发提供的一站式开源软件治理服务，凝聚华为在开源治理上的优秀实践经验，提供开源软件元数据及软件成分分析，从合法合规、网络安全、供应安全等维度消减开源软件使用风险，助力企业更加安全、更加高效地使用开源软件。

检测能力

- 二进制成分分析

  对用户提供的二进制软件包/固件进行全面分析，通过解压获取包中所有待分析文件，基于组件特征识别技术、静态检测技术以及各种风险检测规则，获得相关被测对象的组件BOM清单和潜在风险清单，并输出一份专业的分析报告。

2 功能特性

开源治理服务提供端到端的专项安全检测能力和开源软件元数据管理能力，功能特性如下：

- 二进制成分分析
  - 全方位风险检测

    对软件包/固件进行全面分析，基于各类检测规则，检测相关被测对象的开源软件漏洞和许可证合规、敏感信息（弱口令、硬编码密码等）、安全配置、安全编译选项等存在的潜在风险。
  - 支持各类应用

    支持对桌面应用（Windows和Linux）、移动应用程序（APK、IPA、Hap等）、嵌入式系统固件等的检测。
  - 专业分析指导

    提供全面、直观的风险汇总信息，并针对不同的扫描告警提供专业的解决方案和修复建议。

3 产品优势

- 二进制成分分析
  - 无源码、无侵入快速检测
    只需要上传产品发布包或固件，无需构建运行环境或运行程序。
  - 多语言、多文件格式、多架构平台
    支持多语言，多构建场景下的制品检测，场景覆盖不遗漏。
  - 敏感信息检测防泄露
    支持安全配置和密码密钥等敏感信息检测，发现潜在的安全风险。

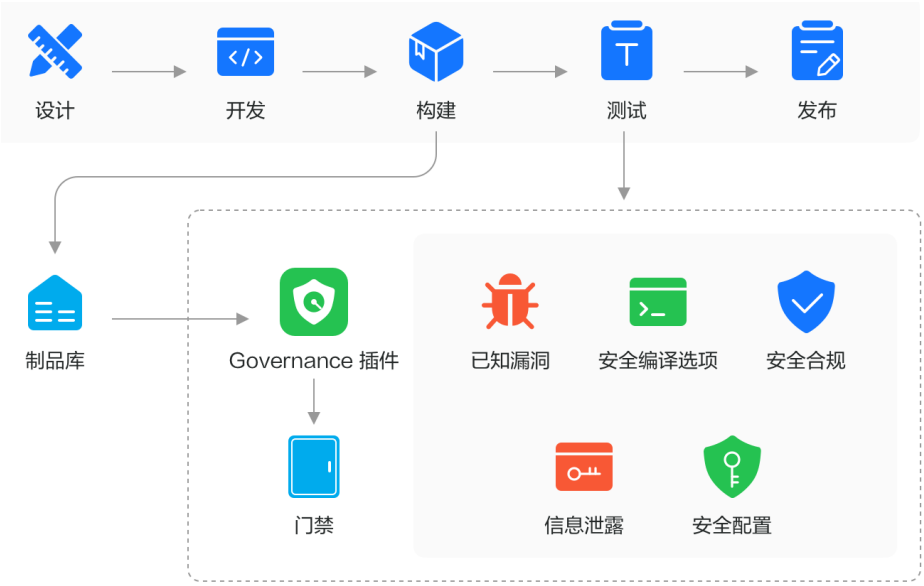
4 应用场景

- 二进制成分分析

  二进制成分分析主要用于以下场景。

  - 开源软件使用风险评估

    二进制成分分析服务提供开放API，并与CI/CD融合，完善DevSecOps安全能力。

  - 开源/第三方软件引入评估

    二进制成分分析服务提供页面和开放API，提供风险快速评估能力。

5 安全

5.1 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5-1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 5-1 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5-1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。

5.2 身份认证与访问控制

身份认证

用户访问CodeArts Governance的方式有多种，包括CodeArts Governance用户界面、API、SDK，无论访问方式封装成何种形式，其本质都是通过CodeArts Governance提供的REST风格的API接口进行请求。

CodeArts Governance的接口需要经过认证请求后才可以访问成功。

CodeArts Governance支持两种认证方式：

- Token认证：通过Token认证调用请求，访问CodeArts Governance用户界面默认使用Token认证机制。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

访问控制

CodeArts Governance服务对接了统一身份认证服务（Identity and Access Management，IAM）服务。CodeArts Governance服务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CodeArts Governance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CodeArts Governance服务资源的访问范围。CodeArts Governance服务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CodeArts Governance服务资源的权限访问控制。

5.3 数据保护技术

CodeArts Governance通过多种手段保护数据安全。

数据保护手段	简要说明
传输加密（HTTPS）	为保证数据传输的安全性，CodeArts Governance使用HTTPS传输数据。
个人数据保护	通过控制个人数据访问权限以及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	CodeArts Governance不消费、不存储用户敏感数据。
数据销毁	用户主动删除业务数据或销户的情况下： • 非关键数据会实时物理删除。 • 关键数据会被标记软删除后，15天再后物理删除。

5.4 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CodeArts Governance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**。

CTS支持追踪的CodeArts Governance操作列表，请参见支持**云审计的操作列表**。

日志

云日志服务（Log Tank Service）提供一站式日志采集、秒级搜索、海量存储、结构化处理、转储和可视化图表等功能，满足应用运维、网络日志可视化分析、等保合规和运营分析等应用场景。

出于分析问题的目的，CodeArts Governance将系统运行的日志实时记录到LTS，并保存3天。

5.5 服务韧性

CodeArts Governance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拉起并修复。

通过以上技术方案，从而保障服务的持久性和可靠性。

5.6 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 5-2 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 5-3 资源中心

6 权限管理

如果您需要对开源治理服务的资源，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云资源的访问。

通过IAM，您可以在云账号中给员工创建IAM用户，并使用策略来控制他们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，您希望他们拥有开源治理服务的使用权限，但是不希望他们拥有删除开源治理服务等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用开源治理服务，但是不允许删除开源治理服务的权限策略，控制他们对开源治理服务资源的使用范围。

如果云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，不影响您使用开源治理服务的其他功能。

IAM是云服务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。请参见**IAM产品介绍**。

开源治理服务权限

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或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

开源治理服务部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，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。访问开源治理服务时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略，策略是角色的升级版。

- 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。由于各云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。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分。

如表6-1所示，包括了开源治理服务的所有系统权限。

表 6-1 开源治理服务系统权限说明

系统角色/策略名称	描述	类别	依赖关系
CodeArtsInspector Administrator	拥有开源治理服务的所有权限。	系统角色	无。
Tenant Administrator	拥有开源治理服务的所有权限。	系统角色	无。

7 约束与限制

介绍开源治理服务的使用限制。

控制台使用限制

表 7-1 控制台使用限制说明

指标类别	指标项	限制说明
浏览器	类型	目前适配的主流浏览器类型包括： ● Chrome浏览器：支持最新的3个稳定版本。 ● Firefox浏览器：支持最新的2个稳定版本。 ● Edge浏览器：Win10默认浏览器。 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。

二进制成分分析使用限制

表 7-2 二进制成分分析使用限制说明

指标类别	指标项	限制说明
任务管理	语言类型	支持C/C++/Java/Go/JavaScript/Python/Rust/Swift/C#/PHP等语言开源软件已知漏洞检测。
	扫描包格式	支持上传.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war、.rpm、.deb等格式文件，以及Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
	扫描包上传大小限制	● 专业版：5GB。 ● 免费版：300MB。

8 产品规格差异

二进制成分分析服务提供免费版和专业版两个版本，其中专业版支持按需套餐包和包年/包月计费模式。相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。

表 8-1 二进制成分分析服务版本规格说明

服务版本	功能特点
免费版	● 每个用户有5次免费体验额度。 ● 扫描文件大小不能超过300MB。 ● 可体验所有检查项功能。 ● 不支持报告下载。 ● 只展示漏洞数排名前10的开源软件信息。
专业版	● 支持查看完整的扫描结果及专业扫描报告导出。 ● 单次扫描最大支持5GB文件。

9 与其他云服务的关系

制品仓库服务

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。

开源治理服务中的开源软件制品资产管理由制品仓库服务提供，用户可以通过超链接跳转至制品仓库服务页面进行查询。

云审计服务

云审计服务（Cloud Trace Service，简称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。

通过CTS，您可以记录与CodeArts Governance相关的操作事件，便于日后的查询、审计和回溯。

10 基本概念

开源软件

开源软件是一种源代码免费向公众开放的软件，任何团体或个人都可以在其许可证的规定下对其进行使用、复制、传播及修改，并可以将该修改形成的软件的衍生版本再发布。

开源软件许可证

所有开源软件都有特定的许可证，可以视为开源软件版权拥有人对开源软件使用者的授权与限制；开源许可证在法律上赋予用户相关权利和义务，任何开源应用行为需要围绕此规则进行。常见的许可证有BSD、Apache、EPL、GPL等，用户选用了相应开源软件，则需要履行相关许可证义务。

扫描报告

开源治理服务中二进制成分分析对用户制品扫描以后生成的扫描结果，用户需要关注如下几种类型的风险结果：

- 开源软件漏洞：用户制品文件中包含的开源软件清单以及相关开源软件版本对应的漏洞信息，用户需要分析是否存在风险以及通过打补丁或升级软件方式进行风险处理。
- 密钥和信息泄露：用户制品文件中包含的疑似敏感信息，如弱口令、硬编码密钥、IP等信息，用户需要结合上下文信息分析是否存在风险。
- 安全编译选项：用户制品文件中编译型语言（如C/C++、Go）的构建产物是否在构建过程中添加对应的保护性编译选项以避免程序运行时受到攻击（如缓冲区溢出攻击等），用户需要结合报告分析有风险文件的构建/编译脚本，添加对应的安全编译选项。
- 安全配置：检测用户制品包中是否存在配置类风险，如凭据类风险、认证问题风险等，用户可基于报告详情中的问题描述和修复指导进行分析处理。
- 开源许可证：用户制品中开源软件包含的许可证清单，部分许可证存在开源风险，而许可证之间也可能会存在兼容性问题，同时引用互斥许可证软件会导致违反开源协议，需用户关注。