代码检查

产品介绍

文档版本 03

发布日期 2025-01-22

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 什么是代码检查

代码检查（CodeArts Check）是基于云端实现的代码检查服务。建立在多年自动化源代码静态检查技术积累与企业级应用经验的沉淀之上，为用户提供代码风格、通用质量与网络安全风险等丰富的检查能力，提供全面质量报告、便捷闭环处理问题，帮助企业有效管控代码质量，助力企业成功。

产品形态包括：云服务和IDE插件。同时，还提供具有深度检查能力的代码检查安全增强包。

云服务代码检查功能列表

表 1-1 云服务代码检查功能列表

功能	描述
编码问题检查	用编码问题检查规则集，对自己的代码进行编码问题缺陷检查。
代码安全检查	用代码安全检查规则集，对自己的代码进行代码安全风险和缺陷检查。
代码风格检查	用代码风格检查规则集，检查自己的代码是否匹配选定风格。
代码健康度评分	一个综合性统一指标，与告警影响度、告警数量、代码量都有关系。自动计算代码健康度分数。
问题管理	通过问题管理中的问题描述、问题状态、检查规则、文件路径、源码以及修改建议等，对检查出来的问题进行处理。
代码圈复杂度	通过代码圈复杂度报表评估代码质量风险。
NBNC代码行	代码检查支持扫描的文件代码行，不包括空行和注释行。
代码重复率	通过代码重复率报表评估代码质量风险。
定时执行检查	提供每周、每日定时检查代码功能，让用户休息编译两不误。

功能	描述
检查结果通知	检查完成后，通过消息通知相关人员检查结果，便于进行及时处理。
多种语言的代码检查	包括Java/C++/JavaScript/Go/Python/C#/TypeScript/CSS/HTML/PHP/LUA/RUST/Shell/KOTLIN。

CodeArts Check IDE 插件介绍

CodeArts Check IDE插件致力于守护开发人员代码质量，成为开发人员的助手和利器。

- 本IDE插件秉承极简、极速、即时看护的理念，提供业界规范（含华为云）检查、代码风格一键格式化及代码自动修复功能。
- 打造了代码检查“快车道”，实现精准、快速检查前移，与Check云端服务共同构筑了三层代码防护体系。
- 内置的轻量级扫描规则作为云端规则的子集，可以在云端查看到所有IDE端规则，实现安全扫描左移，并且覆盖了30多种缺陷分类。
- 当前CodeArts Check IDE插件支持Java、C、C++、Python，并已上线4个主流IDE平台：VSCode IDE、Intellij IDEA、CodeArts IDE、Cloud IDE。

代码安全检查增强包介绍

华为代码安全检查增强包里安全检查能力作为深度价值特性，能深度识别代码中安全风险和漏洞，提供了套餐包内规则不覆盖的安全类场景，比如数值错误、加密问题、数据验证问题等。针对业界的安全漏洞检测项提供了更深入的分析能力，比如，跨函数、跨文件、污点分析、语义分析等。

当前代码安全检查增强包一共有284条规则，涵盖Java语言61个, C++ 语言199个, Go语言8个, Python语言16个。

代码安全检查增强包里安全检查能力支持的检查项如下：

- 覆盖符合污点分析传播模型的漏洞检查，如命令注入、SQL注入、路径遍历、信息泄露等。
- 覆盖业界常见的安全漏洞检测项，如命令注入、LDAP注入、SQL注入、开放重定向漏洞、数值处理、信息泄露等。
- 支持密码、API秘钥和访问令牌硬编码检查能力。
- 支持AcessKey泄露检查。

如果某租户购买了1个增强包，该租户账号及其所有IAM账号均可使用所有增强包相关的规则。

代码安全检查增强包对于扫描次数和扫描的代码行数没有任何限制，仅对代码检查任务并发数有限制，即，买1个增强包代表该租户账号可以扫描1个安全增强特性包规则的代码检查任务，其余任务需要排队等待；买2个增强包表示可同时扫描2个代码检查任务 ……买n个增强包表示可同时扫描n个代码检查任务。当前最多可以买100个。购买方法可参考**购买增值特性**。

增强包不可单独购买，需要在**购买了专业版或企业版CodeArts**之后才会生效，如果购买的CodeArts套餐过期，代码检查特性增强包会失效。

2 产品特性

2.1 自研代码检查引擎

自研代码检查引擎，全面评估代码质量七特征

代码检查服务的核心就是代码检查引擎，高效精准的代码检查引擎能够很好地帮助用户在开发早期快速、准确地发现代码问题，兼顾开发效率与产品质量。

- 代码检查引擎团队凝聚了国内40+博士、海外研究所50+专家、国内外10+老师合作成果，经过华为内部（15W+开发人员，日均500亿行扫描）大规模持续使用和打磨而成。
- 覆盖了业界主流开发语言，针对代码的可读、可维护、安全、可靠、可测试、高效、可移植等方面进行全面的分析。
- 融合了多年对代码质量及可信度提升方面持续思考与探索、实践，积累了丰富的检查规则。

2.2 支持五大业界主流标准和华为编程规范

支持五大业界主流标准和华为编程规范，提升产品代码规范度

软件产品的质量问题往往导致产品产生不可接受的运营风险或过度成本，因此在源代码级别建立质量检测措施的标准是非常重要的，业界如ISO/IEC 5055标准、CERT编程规范等。

- 使用代码检查服务，可以对您的代码进行全面的质量检查。
- 支持快速筛选已识别的编程规范问题，支持规范、标准的知识联动，便于用户快速了解问题类别、严重性、详情，从而根据自身项目需要，快速分析和制定修复计划。
- 当前支持的支持业界主流编程标准和优秀实践有：ISO 5055、CERT、CWE、OWASP TOP 10、CWE/SANS TOP 25等。

2.3 支持主流开发语言

支持主流开发语言，内置 3000+检查规则，便于用户开箱即用

代码检查服务支持Java/C++/JavaScript/Go/Python/C#/TypeScript/CSS/HTML/PHP/LUA/RUST/Shell/KOTLIN等10+常见开发语言，满足嵌入式、WEB应用、移动应用等多种开发场景所需。

- 内置多款的开源工具与自研引擎一起提供丰富的检查规则（3000+）。
- 梳理各类场景需要，内置全面检查规则集、关键检查规则集、移动领域规则集、华为编程规范规则集等10+规则集，便于用户开箱即用。
- 用户也可基于规则库定制满足场景专项需求的检查规则集 。

2.4 日均百亿级扫描能力

日均百亿级扫描能力，支持大型企业超大规模代码检查

代码检查具备强大的高并发处理能力，在华为内部，日常15万+软件开发人员高频代码提交增量检查，每日凌晨所有代码仓定时检查，服务日均扫描百亿行级代码。

- 服务通过AZ容灾、跨region级容灾多活、支持过载保护、服务依赖和隔离等一系列高可用特性，实现服务故障自探测、自隔离、自恢复，为大型应用和团队提供可靠支持。
- 针对检查业务峰谷明显的业务特征，通过强大的弹性调度能力，快速高效的调配资源满足业务所需，确保业务高峰0等待。

2.5 一站式问题闭环修复

一站式问题闭环修复，问题修复效率倍增

开发团队实施代码检查活动时通常遇到问题分析和修复成本高（工具问题不易理解、问题分到具体开发人员费时费力、多版本情况下重复处理同一告警令开发人员厌倦工具）导致落地困难，这些原因很大程度影响了开发人员对检查工具的使用积极性。

代码检查服务提供问题分析处理三大能力，帮助开发团队高效、顺畅使用代码检查：

- 问题精准定位到行、提供修复指导（内置编程规范说明、正确示例、错误示例、修复建议），提高问题分析效率。无需对开发人员重复进行规范和修复技能培训。
- 自动根据代码提交信息匹配问题责任人，提高问题分发效率，谁引入、谁修改，业务逻辑了然于胸，同时加强了开发人员的规范和质量意识。
- 自动同步已处理的忽略问题、同一仓库同一误报只需处理一次，提高问题处理效率。

通过上述能力在实践过程中问题分析和修复效率倍增。

2.6 “代码编写、代码合并、版本发布”三层缺陷防护

“代码编写、代码合并、版本发布”三层缺陷防护，兼顾效率与质量

优秀的代码质量保障实践，往往将代码检查融入到开发作业流中，在用户代码编写、代码提交时进行自动化的审计检查，并对团队每日产出的代码进行持续编程规范和质量检查。

- 这一活动实践要求已是安全开发过程SDL、DevSecOps等众多优秀开发模式推荐进行的实践要求。
- 代码检查服务提供丰富的API接口、涵括任务新建、任务设置、任务扫描、任务报告解析等检查业务全流程，支持用户使用接口方式无缝集成到自建CI/CD或者CodeArts，作业数据灵活对接到客户看板，代码质量可视、可管理。
- 同时通过灵活的任务管理，支持排除目录设置避免无效扫描，并支持混合语言检查、简化部署、一次获取整个版本代码质量。

2.7 代码检查安全增强

CodeArts Check提供代码安全检查增强包的能力，其安全检查能力作为深度价值特性，能深度识别代码中安全风险和漏洞，提供了套餐包内规则不覆盖的安全类场景，比如数值错误、加密问题、数据验证问题等。针对业界的安全漏洞检测项提供了更深入的分析能力，如跨函数、跨文件、污点分析、语义分析等。

当前代码安全检查增强包一共有284条规则，涵盖Java语言61个, C++ 语言199个, Go语言8个, Python语言16个。

表 2-1 增强包与普通版本检查能力差异

检测项	OWASP TOP	CWE TOP	详细描述	基础版/专业版	代码安全增强包
命令注入	支持	支持	攻击者利用外部输入构造系统命令，通过可以调用系统命令的应用，实现非法操作的目的。	支持	支持
路径遍历	不支持	支持	攻击者利用系统漏洞访问合法应用之外的数据或文件目录，导致数据泄露或被篡改。	不支持	支持
SQL注入	支持	支持	攻击者利用事先定义好的查询语句，通过外部输入构造额外语句，实现非法操作的目的。	支持	支持
未受控的格式化字符串	不支持	支持	攻击者可利用格式化字符串漏洞实现控制程序行为和信息泄露。	不支持	支持
跨站脚本攻击（XSS）	支持	支持	攻击者利用在网站、电子邮件中的链接插入恶意代码，盗取用户信息。	不支持	支持

检测项	OWASP TOP	CWE TOP	详细描述	基础版/专业版	代码安全增强包
LDAP注入	支持	支持	利用用户输入的参数生成非法LDAP查询，盗取用户信息。	不支持	支持
不安全的反射	支持	支持	攻击者利用外部输入绕过身份验证等访问控制路径，执行非法操作。	不支持	支持
开放重定向漏洞	不支持	支持	攻击者可通过将跳转地址修改为指向恶意站点，即可发起网络钓鱼、诈骗甚至窃取用户凭证等。	不支持	支持
XPath注入	支持	支持	攻击者利用外部输入附带恶意的查询代码，用于权限提升等。	支持	支持
数组索引验证不正确	不支持	支持	造成越界读取内存，可能引发信息泄露或者系统崩溃。	不支持	支持
空指针解引用	不支持	支持	会造成不可预见的系统错误，导致系统崩溃。	支持	支持
日志中信息泄露	不支持	支持	服务器日志、Debug日志中的信息泄露。	不支持	支持
消息中信息泄露	不支持	支持	通过错误消息导致的信息暴露。	支持	支持

3 产品优势

专业

- 提供3000条以上典型检查规则。
- 提供多维度质量统计报表，如质量门禁。

精准

- 精确定位缺陷，提供修复指导。
- 支持用户自定义检查规则集，精准检查用户关注缺陷。

全面

- 支持Java/C++/JavaScript/Go/Python/C#/TypeScript/CSS/HTML/PHP/LUA/RUST/Shell/KOTLIN等多种主流开发语言。
- 支持代码规范检查、安全检查、代码重复率和圈复杂度检查。
- 兼容CWE/HUAWEI/OWASP TOP 10/ISO 5055/SANS TOP 25/CERT/MISRA安全标准。

易用

- 支持多种语言混合检查。
- 配置任务一键执行，批量过滤缺陷，分级分类快速处理。

支持代码安全检查

支持场景

- 软件开发阶段对代码质量和安全问题进行自动化检查，支持内置安全规范、要求到软件生产作业流，帮助企业软件生产安全。
- 提供深度代码安全检查能力，帮助政务云运营者和大企业管控ISV软件安全质量，构建供应链安全体系。

能力说明

- 提供跨函数、跨文件检查能力，提供污点分析检查能力。
- 支持注入类、信息泄露类（AccessKey）等TOP安全漏洞检查。

- 支持编程规范，兼容支持CWE/HUAWEI/OWASP TOP 10/ISO 5055/SANS TOP 25/CERT/MISRA检查。

4 应用场景

Web 应用安全检查

- 应用：使用规则集对Web开发语言进行代码检视，并为开发角色提供修复建议，比如修改的代码位置、系统、语言、模块、引擎等。
- 场景特点：Web服务面向Internet互联网，容易遭受DDos攻击、信息泄露等风险。
- 适用场景：互联网服务交付安全等级验收。

项目质量控制

- 应用：在交付过程中实时根据代码复杂度、重复率、质量得分控制风险。
- 场景特点：项目经理的共识“从前端保证质量，把质量做在日常交付”，但经常没有有效的工具平台，目前大部分的质量工作还是依赖后端测试。
- 适用场景：项目经理迭代交付质量控制。

5 安全

5.1 责任共担

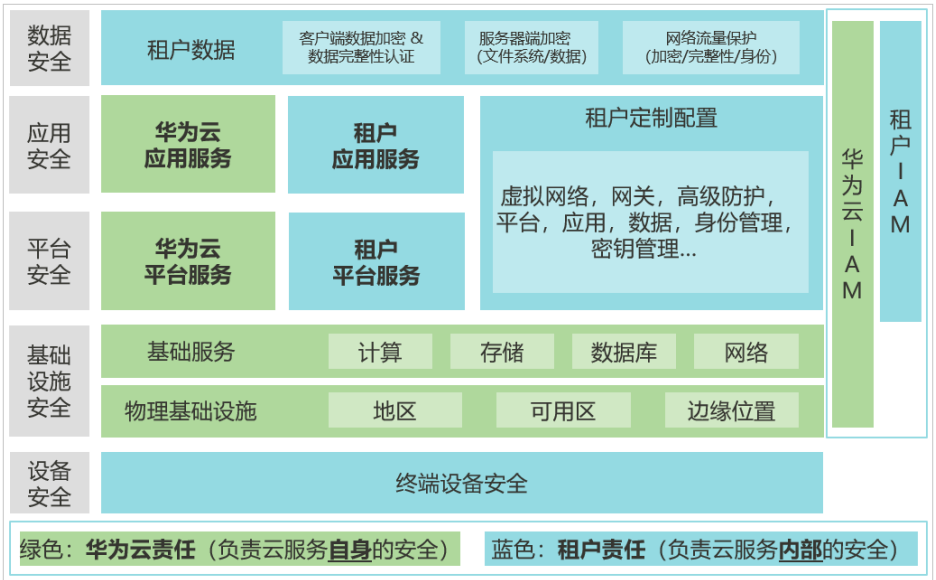
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图5-1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类云服务自身的安全，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 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

身份认证

用户访问代码检查服务的方式有多种，包括代码检查用户界面、API、SDK，无论访问方式封装成何种形式，其本质都是通过代码检查提供的REST风格的API接口进行请求。

代码检查的接口需要经过认证请求后才可以访问成功。代码检查支持两种认证方式：

- Token认证：通过Token认证调用请求，访问代码检查用户界面默认使用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。

  关于认证鉴权的详细介绍及获取方式，请参见**认证鉴权**。

访问控制

代码检查对用户操作进行访问控制的方式如下：

- 角色权限控制：对代码检查任务、规则集的增删改查，规则查看，问题单的创建和导入导出等都均需获得对应的角色及权限。
- 细粒度权限控制：查询租户项目、设置项目创建者、管理租户项目成员列表等操作需要获得IAM细粒度授权。

5.3 数据保护技术

代码检查通过多种数据保护手段和特性，保障数据安全可靠。

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	为保证数据传输的安全性，代码检查使用HTTPS传输数据。	构造请求
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。	权限控制
隐私数据保护	涉及到用户的数据库账号信息需要存储时，提供敏感数据加密存储。	-
数据清理	检查任务执行过程中的敏感数据，检查完成后立即清理。	-
数据备份	支持用户数据备份。	-

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可记录代码检查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**。

5.5 服务韧性

代码检查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。

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 约束与限制

命名限制

限制项	说明
检查任务名称	● 支持中英文，数字，点，下划线“_”和连接符“-”。 ● 字符长度范围为1~128。
规则集名称	● 支持中英文，数字，点，下划线“_”和连接符“-”。 ● 字符长度范围为1~128。

规格与限制

指标项	限制值
单次检查支持扫描的问题数量	一个代码检查任务支持扫描的问题数量最多为300000。
租户自定义规则集数（个）	租户可以自定义的规则集数最大为1000。
租户创建代码检查任务数（个）	租户下可以创建的总任务数最大为50000。
单次代码检查最大时长	12小时。
浏览器	目前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 ● Edge浏览器：Win10默认浏览器，支持和测试最新的3个稳定版本 **推荐**使用**Chrome**、**Firefox**浏览器，效果会更好。
分辨率	推荐使用1280*1024以上。

7 基本概念

表 7-1 代码检查服务基本概念

词汇	定义
重复率	重复行数是指涉及至少一次重复的代码行数；重复块是指包含重复行的代码块（最小重复块定义：Java语言连续10行重复，其它语言10行中连续100个字符重复算一个重复块）；重复率=重复行/代码总行数（不包含空行与注释）。
规则	应用于检查某类代码问题。提供规则说明，如代码缺陷影响、修改建议。
规则集	针对具体语言而定义的检查规则集合，提高用户代码质量。
圈复杂度	圈复杂度是一种代码复杂度的衡量标准，与其可维护性和可测试性之间存在相关性，这意味着在圈复杂度较高的文件中，重构代码出错的概率较高。代码平均圈复杂度 = 总圈复杂度/函数数。具体风险评估建议如下： ● 1~5：低风险 ● 6~10：较低风险 ● 11~20：中等风险 ● 21~50：高风险 ● 51+：极高风险 ● NA：CodeArts Check不支持检查该语言
SDLC	软件开发生命周期（Software Development Life Cycle）。
问题展示	准确定位到问题所在代码行，用户可以在线查看并分析代码问题。
延迟上线	在工具版本升级后，由于代码检查服务检查引擎的能力提升，可能会出现新的缺陷。但新检查出来的缺陷，不会计算到正式缺陷中，开发者拥有60天的缓冲周期对代码进行修改，周期内没有修改或者屏蔽的缺陷，在周期结束后后会计算到正式缺陷中。
执行计划	定义代码检查任务自动触发的方式。通过触发器，使代码检查的自动化执行更加灵活易用。