代码检查

常见问题

文档版本	04
发布日期	2023-12-01

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。

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 一般问题

1.1 代码检查角色权限

角色权限表

针对项目下资源（任务、规则集等），介绍代码检查中用户默认的角色权限说明，如**表 代码检查默认角色权限说明**所示。

表 1-1 代码检查默认角色权限说明

资源权限/角色		项目管理员	项目经理	开发人员	测试经理	测试人员	项目参与者	浏览者	运维经理	产品经理	系统工程师	Committer
代码检查任务	创建	√	√	√	×	×	×	×	×	×	√	√
	执行	√	√	√	×	×	×	×	×	√	√	√
	查看	√	√	√	×	×	×	×	×	√	√	√
	修改	√	√	√	×	×	×	×	×	√	√	√
	删除	√	√	×	×	×	×	×	×	√	√	√

资源权限/角色		项目管理员	项目经理	开发人员	测试经理	测试人员	项目参与者	浏览者	运维经理	产品经理	系统工程师	Committer
规则集	设置默认规则集	√	√	×	×	×	×	×	×	√	√	√
缺陷报告	查看	√	√	√	×	×	×	×	×	√	√	√
	修改	√	√	√	×	×	×	×	×	√	√	√
	导出	√	√	√	×	×	×	×	×	√	√	√

1.2 如何使用代码检查?

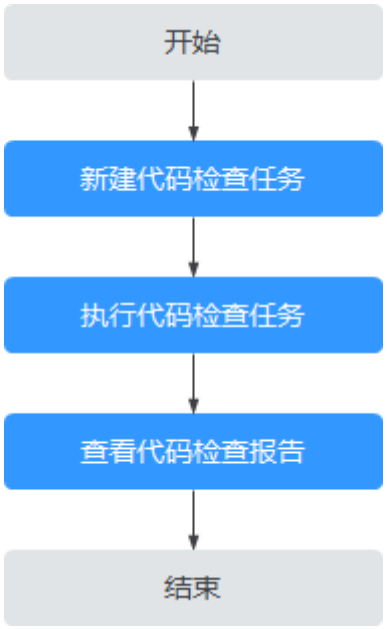
背景信息

代码检查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、便捷的问题闭环处理帮助企业有效管控代码质量，助力企业成功。

操作流程

介绍代码检查的基本使用流程。

图 1-1 基本使用流程



流程说明

流程	说明
新建代码检查任务	在CodeArts首页选择“服务 > 代码检查”，单击“代码检查”首页“新建任务”可以新建代码检查任务。
执行代码检查任务	代码检查任务新建成功后，进入任务详情页或在任务列表页面，单击“开始检查”。
查看代码检查报告	检查完成后，可以查看任务详情，如：“概览”、“代码问题”、“代码度量”、“检查日志”和“设置”。

1.3 代码检查支持哪些区域?

代码检查服务目前支持以下区域：

- 拉美-墨西哥城二
- 拉美-圣保罗一
- 亚太-新加坡

1.4 代码检查能够检查哪些语言?

目前支持Java、C++、JavaScript、TypeScript、C#、Python、PHP、Go、HTML、CSS、LUA、RUST、Shell，其他语言类型，敬请期待！

1.5 代码检查能够检查哪些维度?

代码检查主要从“编码风格”、“编码问题”、“编码安全”和“架构设计”方面对源代码进行检查分析，上报代码缺陷，并分析源代码的“圈复杂度”和“代码重复率”，根据检查结果评定代码风险指数并提出修改建议。

1.6 代码检查能否检查本地代码?

不能。

代码检查不能单独使用，需要配合云端代码仓。

代码检查服务仅适用于云端代码仓库，需要将本地代码提交到云端代码仓库后，才能进行云端代码检查分析。

1.7 代码检查是检查代码执行的 Bug 吗?

不是。

代码检查服务是对代码仓库中的指定源代码进行静态分析，即在不运行代码的情况下，通过词法分析、语法分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标。同时，对分析出的代码缺陷提供示例与修改建议。

1.8 代码检查缺陷如何定位到代码提交者?

目前代码检查结果只能定位到某一行代码、及对应的代码文件，不能直接定位到代码提交者，可以通过代码仓库中的提交记录查看哪位成员修改过文件，进而定位到代码的提交者。

说明

在项目成员提交代码前，请先执行代码检查任务，修改无误后再提交合并。

1.9 一个代码检查任务是否能选择多个规则集?

可以。

一个任务的规则集取决于仓库中代码的种类，多种语言就可以选择多种规则集，但是一种语言只能选择一种规则集。

1.10 如何导出代码问题?

步骤1 进入代码检查详情页，选择“代码问题”页签。

步骤2 在页面左侧过滤器中筛选需要导出的代码问题，如“问题级别”或“问题状态”。

步骤3 勾选目标问题，单击页面下方“导出”，可以导出已选中的目标代码问题。

----结束

2 使用代码检查

2.1 任务正在执行，稍后重试

问题现象

执行任务失败，提示异常信息：任务正在执行，稍后重试。

原因分析

该任务正在运行，造成流水线执行失败。

处理方法

步骤1 从流水线中进入当前代码检查任务中。

步骤2 确认当前任务是否正在运行，如果在执行请等待执行完成后，再开始运行流水线。

如果仍然未能解决，请联系技术支持工程师。

----结束

2.2 权限不足，请核对后再试

问题现象

执行任务失败，提示异常信息：权限不足，请核对后再试。

原因分析

当前用户操作权限不足，无法操作该任务，请用户根据权限矩阵，核对并联系项目管理员（项目创建者、项目经理）更改当前账号权限。

处理方法

步骤1 进入项目“成员管理”页面，查看自己的项目角色权限。

步骤2 根据**权限矩阵**，联系项目的管理员修改自己需要的“项目角色”。

----结束

2.3 Cppcheck cannot tokenize the code correctly

问题现象

代码检查提示“Cppcheck cannot tokenize the code correctly”。

原因分析

是Cppcheck的一条检查规则，在代码里面有语法错误，用Java语法写C代码造成的。

处理方法

要按照C语言的编码规范写代码，不能包含其他语言的编码规则。

2.4 任务执行检查完毕后没有数据

问题现象

任务执行检查完毕后没有数据。

原因分析

- 源代码仓语言没有获取到。
- 检查语言开关没有打开。

处理方法

步骤1 进入任务“设置 > 规则集”页面。

步骤2 单击“已包含语言”所在行 重新获取代码仓语言。

步骤3 打开需要检查语言的开关。

步骤4 重新执行检查。

----结束

2.5 使用公共 API 报没有权限

问题现象

使用公共API报没有权限。

原因分析

- 登录的用户没有权限。
- Region信息不对。

处理方法

步骤1 确认登录的用户是否有权限，详情见**权限矩阵**。

步骤2 确认Region信息是否正确。

如果仍然未能解决，请联系技术支持工程师。

----结束

2.6 使用公用 API 提示项目不存在

问题现象

使用公用API提示项目不存在。

原因分析

taskId错误导致。

处理方法

使用正确的taskId。如果仍然未能解决，请联系技术支持工程师。

2.7 编译参数设置

JAVA 语言任务

选用全面规则集、安全规则集时，需要设置检查参数，用于编译结果文件检查。

步骤1 进入任务“设置 > 规则集”页面。

步骤2 单击“已包含语言”所在行 重新获取代码仓语言。

步骤3 单击“检查参数”按钮。

步骤4 选择Java编译工具、编译工具版本，输入编译命令。

步骤5 在“检查参数”窗口中打开启用开关，单击“确认”。

----结束

2.8 TypeScript 任务检查失败

问题现象

TypeScript任务检查失败，日志显示404。

处理方法

请检查上传的项目文件中是否包含“package-lock.json”文件。

- 如果包含，则删除“package-lock.json”文件，重新Push代码进行检查。
- 如果不包含，则联系技术支持工程师。

3 安全性

3.1 代码检查如何保证客户代码安全?

账号由IAM统一认证，每个项目均设有权限管理机制，项目管理员才可以管理项目成员。更多安全资讯请参见**信任中心**。

3.2 代码检查是否可检查 SQL 注入等安全问题?

是。

代码检查支持编码风格、编码问题、编码安全、架构设计等功能，其中编码安全中支持检查SQL注入、XML外部实体注入攻击、潜在LDAP注入攻击、潜在的Xpath注入攻击等。

4 高阶问题

4.1 代码检查特性增强包里有哪些规则?

用户在购买了代码安全检查增强包后，可以使用安全维度更为深度的缺陷扫描能力，包含100多条专属规则，当前涵盖Java、C++、Go和Python。

安全检查增强包提供跨函数、跨文件、污点分析、语法树搜索、语义分析等专业的代码安全检查能力，能深度识别代码中的安全风险和漏洞。

表 4-1 代码安全检查增强包

计费方式	包年/包月
适用场景	代码检查服务提供了100+条代码安全检查增强包规则，使用这些规则时需购买代码安全检查增强包。
资源规格	1个并发
购买限制	● 购买代码安全检查增强包前，须完成CodeArts基础版的购买。 ● 购买上限为100个。
计费公式	单价*数量*购买时长
计费周期	根据购买时长确定（以GMT+08:00时间为准）。一个计费周期的起点是您开通或续费代码安全检查增强包的时间（精确到秒），终点则是到期日的23:59:59。 例如，如果您在2023/03/08 15:50:04购买时长为一个月的代码安全检查增强包，那么其计费周期为：2023/03/08 15:50:04 ~ 2023/04/08 23:59:59。
变更配置	不支持变更配置。若完成购买后发现配置有误，需退订后重新购买。
到期后影响	到期未续费时，该代码安全检查增强包中包含的并发数将失效。

4.2 代码检查怎么创建自定义规则集?

在“规则集”标签页面里，选择“新建”按钮，然后输入规则级名称，描述（可选），选择检查语言，继承/复制于现有某个规则集（可选）。

单击“确定”，即跳转到规则集详情页面，可以根据需要勾选对应规则、还可以自定义规则的级别，然后单击右上角“保存”。

4.3 代码检查的规则集可以修改名称吗?

系统默认规则集不可以修改名称，自定义规则集可以修改名称。

进入代码检查规则集列表，单击要修改的规则集。在规则集详情页面，单击右上角“修改基本信息”，编辑规则集名称，单击“确定”即可完成名称修改。

4.4 新建的检查任务不能删除，要运行之后才能删除?

代码检查服务中新建的检查任务可以直接删除。

4.5 代码检查只能使用 CodeArts Repo 服务才能使用吗?

不是。代码检查配合云端代码仓就可以使用。当前支持的云端代码仓服务有：CodeArts Repo代码托管、GitHub、码云和通用Git代码仓。

4.6 当前 CodeArts Check 支持哪些本地 IDE 编辑器?

当前支持VSCode IDE、JetBrains IDEA、CodeArts IDE Online（线上），并已上线4个主流IDE平台：VSCode IDE、Intellij IDEA、CodeArts IDE、Cloud IDE。

