开源治理服务

最佳实践

文档版本 01

发布日期 2025-09-29

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 CodeArts Governance 最佳实践汇总

本文汇总了基于开源治理服务（CodeArts Governance）常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户了解CodeArts Governance的使用方法。

表 1-1 CodeArts Governance 最佳实践一览表

最佳实践	说明
使用CodeArts Governance进行二进制成分分析	本实践为您介绍如何使用CodeArts Governance进行二进制成分分析。
通过流水线自动完成CodeArts制品产物二进制成分分析	本实践为您介绍通过流水线自动完成CodeArts制品产物二进制成分分析。

2 使用 CodeArts Governance 进行二进制成分分析

应用场景

据《2024年中国软件行业全景图谱》统计，2023年国内软件市场规模超12万亿，我国软件行业正处于成长期，市场规模增长较快，预计2029年整体行业的市场规模将超21万亿。据《2023年软件供应链状况报告》指出，过去三年针对软件供应链的攻击平均年增长高达742%。因此，开源/第三方软件引入评估面临以下问题：

- 针对采购的软件或对外交付的软件产品没有很好的安全检测手段。
- 产品需要对供应商有基础的安全性认证。
- 开源漏洞响应与修复效率低，安全风险缺乏管理。

通过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。功能特性如下：

- 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。
- 恶意代码检查：提供病毒木马等恶意软件的扫描，支持开源软件中敏感信息外发、木马下载执行、反弹shell、恶意命令执行恶意行为检测。

方案架构

以下示意图为用户申请开源/第三方软件场景，该软件包含制品包，将制品包提供给二进制成分分析服务进行检测，检测项包括：已知漏洞、安全编译选项、信息泄露、安全配置、恶意代码/软件等风险项，并输出风险评估报告，待风险项完成整改后进行使用。

方案优势

- 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。
- 恶意代码检测，确保供应安全
  基于AI开源软件恶意代码检测能力，恶意行为早发现。
- 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。

约束与限制

表 2-1 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。

实施步骤

步骤1 登录开源治理服务控制台。

步骤2 在左侧导航栏，单击“软件成分分析 > 二进制成分分析”。

步骤3 在“二进制成分分析”页面，单击“添加任务”，弹出“添加任务”对话框，单击“扫描对象”旁的文件框，选择本地的软件包，导入扫描对象。

表 2-2 参数说明

参数	参数说明
扫描对象	待扫描的软件包/固件。
任务名称	扫描文件的名称。
检查项	勾选需要分析的检查项。 **说明** 选择一个或者多个检查项，都视为一次扫描，按照一次扫描扣费。
任务描述	对任务信息进行说明。
是否将本次扫描升级为专业版规格	当计费模式不是包年/包月，且免费版有剩余次数时涉及该参数。 ● 关闭开关，本次扫描使用免费版配额。 ● 打开开关，可以将本次扫描升级为专业版规格。升级后，您本次扫描可享受专业版规格，包含如下额外功能：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。如果您扫描次数较为频繁，建议您购买包年专业版服务。

步骤4 文件上传成功后，单击“确定”，等待扫描任务完成。

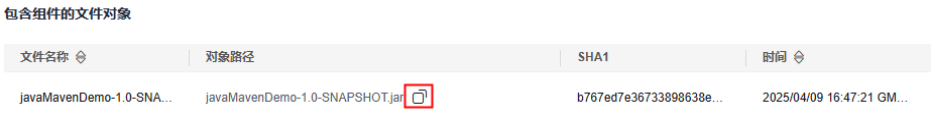
步骤5 单击任务名称，也可以单击任务列表操作列的“查看报告”，进入扫描报告页面。扫描报告页面说明如表2-3所示。

表 2-3 详情总览说明

栏目	说明
任务概况	• 显示目标任务的基本信息，包括：文件名、文件大小、特征库版本、平台版本等基本信息。 • 显示目标任务的组件检测、安全漏洞、安全配置、开源许可证、信息泄露、安全编译选项、恶意软件扫描检测概况，包括： – 组件检测：展示被扫描的软件包所有的组件数量，有漏洞、未知版本和无漏洞组件数量占比。 – 安全漏洞：展示超危、高危、中危、低危各个级别漏洞数量占比。 – 安全配置：展示通过、失败、不涉及的检测结果数量占比。 – 开源许可证：展示高风险、中风险、低风险各个级别开源许可证的统计信息。 – 密钥和信息泄露：展示信息泄露各检测项结果分布。 – 安全编译选项：展示安全编译各检测项结果分布。 – 恶意软件扫描：展示病毒和恶意代码扫描结果分布。
开源软件漏洞	显示扫描任务中每个组件的组件名称、组件版本、开源许可证、包含文件数以及存在漏洞数。 • 组件名称、组件版本和文件数可按升降序查看。 • 可按组件名称、开源许可证对组件列表进行筛选查看。
开源许可证	显示开源软件的许可证检测结果，包括许可证使用的集成风险和许可证间的兼容性风险。 • 许可证信息：二进制文件包许可证检测结果，包含许可证名称、集成风险、涉及组件和许可证描述和风险分析。 • 许可证兼容性：二进制文件包中各目录的许可证间兼容性风险检测。
密钥和信息泄露	显示Git地址、IP、硬编码密码、弱口令、硬编码密钥和SVN地址的检测结果。
安全编译选项	显示BIND_NOW、NX、PIC等检测项目的描述、检测结果、不符合文件数。
安全配置	显示凭据管理、认证问题和会话管理的检测项目、安全风险等级、检测结果。
恶意软件扫描	显示病毒扫描和恶意代码扫描的结果。

- 在“开源软件漏洞”页签可查看软件包各个组件的漏洞。
  如果检测结果存在漏洞或者风险，可单击“组件名称”列，查看详细信息。
  – 单击“对象路径”后的  ，可以复制文件对象路径详细信息。

图 2-1 复制文件对象路径



  - 单击“CVE”漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“解决方案”、“漏洞修复参考”、“参考链接”。
- 在“密钥和信息泄露”页签查看对应检测项目的检测结果。
- 在“安全编译选项”页签查看编译选项对应检测项目的检测结果。
- 在“恶意软件扫描”页签查看病毒扫描和恶意代码扫描的检测结果。

----结束

3 通过流水线自动完成 CodeArts 制品产物二进制成分分析

应用场景

随着软件功能的不断扩大，软件面临的安全风险也在增加，如何快速精准地识别软件安全风险成了一大难题。

- 传统方式需要用户打包后再手动上传软件包进行扫描，然后查看扫描结果获取软件漏洞信息，过程繁琐。
- 不同的软件漏洞风险影响不同，需手动识别。

通过搭建流水线，可实现从代码仓到获取软件漏洞结果的整个流程，同时可以通过配置不同的准出条件，对软件漏洞实现分级管理。

方案优势

- 搭建简单，无需重复配置

  只需在搭建流水线时配置一次，即可重复实现完成修改代码、构建出包、漏洞扫描的完整流程。
- 漏洞风险分级治理

  支持配置准出条件，实现对不同风险等级软件漏洞的分级管理并对扫描结果进行拦截。

约束限制

流水线可配置定时任务或外部触发执行，为避免不必要的扫描次数浪费，使用插件需要购买二进制成分分析包周期版本，暂时不支持购买按需套餐包的用户使用插件。

操作流程

本文介绍如何通过流水线完成代码修改、构建出包、漏洞扫描的全过程，基本操作流程如下：

步骤1：新建规则和策略

步骤2：新建Scrum项目

步骤3：新建代码仓库

步骤 1：新建规则和策略

步骤1 登录华为云官网，单击页面右上角“控制台”。

步骤2 在页面左上角单击，打开服务列表。

步骤3 搜索“流水线”。

步骤4 单击“流水线 CodeArts Pipeline”，进入流水线服务首页。

步骤5 单击右上角头像图标，在下拉菜单中选择“租户设置”，进入租户设置页面。

步骤6 单击左侧导航“策略管理 > 规则”，进入规则管理页面。

步骤7 单击“新建规则”，进入“新建规则”页面，配置以下信息。

表 3-1 配置规则信息

参数项	说明
名称	规则名称，使用自动生成的即可。
类型	规则类型，选择“测试”。
选择插件	规则绑定的插件名称，选择“二进制软件成分分析”。
插件版本	规则绑定的插件版本，不同插件版本输出的阈值可能有差异，例如选择“1.0.0”。
阈值配置	配置检查项阈值，例如图3-1所示。

图 3-1 新建规则

步骤8 单击“确定”，完成规则创建。

步骤9 单击左侧导航“策略”，进入策略管理页面。

步骤10 单击“新建策略”，进入“新建策略”页面，输入策略名称，勾选新建好的规则。

步骤11 单击“确定”，完成策略创建。

----结束

步骤 2：新建 Scrum 项目

步骤1 单击顶部导航栏“首页”。

步骤2 在所有项目下单击“Scrum > 新建项目”。

步骤3 选择“Scrum”项目模板，单击“选用”，进入新建项目页。

步骤4 项目名称填写“Scrum01”，其它保持默认即可。

步骤5 单击“确定”后，进入到“Scrum01”项目下。

----结束

步骤 3：新建代码仓库

步骤1 在页面导航栏选择“代码 > 代码托管”，进入代码托管页面。

步骤2 单击“新建仓库”，选择“按模板新建”。

步骤3 单击“下一步”，选择“Java Maven Demo”模板。

步骤4 单击“下一步”，填写仓库名称。

步骤5 单击“确定”，完成代码仓库的创建。

----结束

步骤 4：新建编译构建任务

步骤1 在页面导航栏选择“持续交付 > 编译构建”，进入编译构建页面。

步骤2 单击“新建任务”，根据需要配置任务信息。

1. 配置基本信息：填写任务名称，选择Repo代码源，选择**已创建的代码仓库**，选择默认分支master，单击“下一步”。
2. 选择构建模板：选择Maven系统模板，单击“确定”，进入“构建步骤”页面，使用默认配置即可。

步骤3 单击“保存”，完成构建任务的创建。

----结束

步骤 5：新建流水线

步骤1 在页面导航栏选择“持续交付 > 流水线”，进入流水线页面。

步骤2 单击“新建流水线”，根据需要配置流水线信息。

1. 基本信息：配置以下信息，单击“下一步”。

表 3-2 流水线基本信息

配置项	配置建议
名称	流水线名称，使用默认生成的即可。
代码源	选择“Repo”。
代码仓	选择**已创建的代码仓库**。
默认分支	选择“master”分支。

2. 选择模板：选择“空模板”，单击“确定”。

步骤3 进入“任务编排”页面，系统默认生成两个阶段（“流水线源”和“阶段_1”），单击“新建阶段”新增一个阶段“二进制成分分析”。

1. 配置构建阶段
   a. 单击“阶段_1”的“新建任务”，弹出“新建任务”侧滑框。
   b. 单击“构建”分类，找到“Build构建”插件。
   c. 将鼠标移动到插件，单击“添加”，选择**已创建的构建任务**，选择构建任务关联的仓库，产物标识输入“javaSample”。
   d. 单击“任务配置”，将任务ID设置为“build”。
   e. 单击“确定”，完成任务配置。
2. 配置二进制成分分析阶段
   a. 单击“二进制成分分析”阶段的“新建任务 > 从空任务新建”，弹出新建任务侧滑框。
   b. 单击“通用”分类，找到“下载制品产物”插件。
   c. 将鼠标移动到插件，单击“添加”，产物链接输入“${{jobs.build.artifacts.javaSample}}”。
      - “build”为构建阶段中设置的任务ID。
      - “javaSample”为构建阶段中“Build构建”插件中设置的产物标识。
   d. 单击“添加步骤”，在“测试”分类找到“二进制软件成分分析”插件，使用默认配置。
   e. 单击“确定”，完成任务配置。
   f. 单击“二进制成分分析”阶段的“准出条件”，在弹出的侧滑框里添加准出条件，将鼠标移动到“标准策略准出条件”上，单击“添加”，并选择**已创建好的策略**。
   g. 单击“确定”，完成准出条件配置。

步骤4 任务编排完成后，单击“保存并执行 > 执行”，开始执行流水线。

----结束

步骤 6：查看插件执行结果

步骤1 流水线执行完成后，进入详情页面。

步骤2 单击“二进制成分分析”阶段的“下载制品产物”任务，弹出侧滑框。

步骤3 在侧滑框的“任务日志”页面，单击“详情”，页面跳转到开源治理服务对应构建包的扫描详情页面，即可查看扫描结果。

步骤4 在侧滑框的“任务结果”页面，单击“二进制软件成分分析”可以直接查看部分扫描结果。

步骤5 单击准出条件，可查看扫描结果是否满足设置的规则，从而控制流水线执行。

- 当扫描结果满足条件时，流水线继续执行。
- 当扫描结果不满足条件，流水线停止执行。

----结束