openEuler社区门禁、合规检查梳理优化

openEuler Infrastructure SIG / Compliance SIG

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

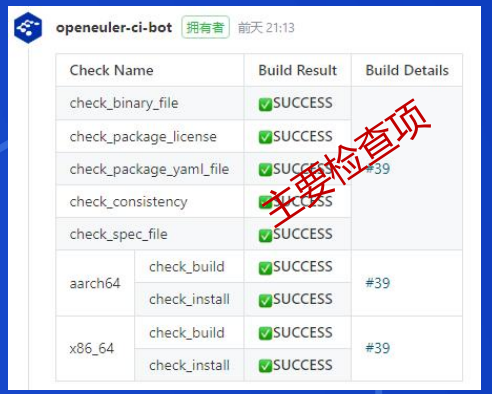
背景

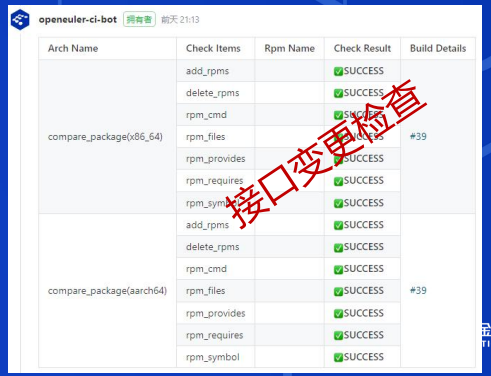
1. 门禁检查项目逐步增加，相关检查项是否作为“合入控制点”存在异议；
2. 门禁没有统一纳管相关检查项，没有统一向开发者呈现检查结果；
3. 检查项内容不太透明，检查项判断标准未明显展示；
4. openEuler版本安全扫描检查出一些不符合license准入清单要求的license；

当前门禁检查项

检查类型	检查项	功能	判断标准	结果	评论	标签
静态检查	check_binary_file	检查仓库中是否存在二进制文件	不存在以.pyc、.jar、.ko、.o为后缀的文件（包括压缩包内，但不包括以链接形式给出的上游社区）	通过	√SUCCESS	不影响
				未通过	×FAILED	不影响
	check_package_license	检查license合法性	有license并且全部为白名单，并且源码和spec描述的license保持一致，也存在项目级copyright文件	通过	√SUCCESS	不影响
				未通过	×FAILED	不影响
				Copyright缺失	！ Warning	不影响
	check_package_yaml_file	检查yaml格式	version_control、src_repo、tag_prefix、seperator字段完整，并且version_control字段内容与spec文件中url对应的域名一致	通过	√SUCCESS	不影响
			评论：success 标签：不涉及	不通过	×FAILED	不影响
	check_spec_file	检查sepc合法性	版本号不变时，release号必须递增；版本号变化时，release必须置为1；补丁在编译时必须全部应用；changelog格式正确	通过	√SUCCESS	不影响
				不通过	×FAILED	不影响
	check_consistency	校验源码文件一致	通过远端和本地源码文件的sha256值是否一致来判断源码包是否发生变更	通过	√SUCCESS	不影响
				不通过	×FAILED	不影响
				本地数据缺失	！ Warning	不影响
构建&安装	check_build	验证编译	构建rpm包成功，当前含X86和aarch64	通过	√SUCCESS	ci_successful
				不通过	×FAILED	ci_failed
	check_install	验证安装	安装构建出的rpm包，当前含X86和aarch64	通过	√SUCCESS	ci_successful
				不通过	×FAILED	ci_failed
接口变更	Compare_package	接口变更检查	本次pr编出的包和上次pr编出的包没有出现接口变更差异信息	通过	√SUCCESS	不影响
			评论：success 标签：不涉及	不通过	×FAILED	不影响

1.静态检查、接口变更结果不在标签体现，仅在评论钟呈现；
2.标签会根据构建、安装、及软件包归档的结果呈现；
3.不论评论还是标签的fail目前都没有成为合入流程硬性控制点；





当前合规检查实现

检查项	功能	基线规则	动作	结果	最佳实践
Repo License	Repo缺乏整体的License	在根目录（license、readme、copyright、notice 等）或者 1 层子目录（/License(s)/License, Notice/License 等)下有文件中有 License 的完整文本的说明。	获取PR合入目标代码，分析前两层子目录下**是否存在License文件**声明	**SUCCESS**：Repo存在License声明 **FAILED**：Repo不存在License声明	建议使用以下两种方式之一： 1.在根目录下放单独的 License 文件。 2.在 Licenses/License 子目录下放单独的完整 License 文件。
Spec文件License	Repo spec文件的License不规范	License名称清晰、规范性，不产生歧义	提取PR合入目标代码SPEC文件，分析**License声明是否缺失、规范**	**SUCCESS**：spec文件License声明清晰规范、不存在歧义 **FAILED**：spec文件License声明不清晰、不规范、存在歧义	使用统一格式的 spdx-indentifier
非准入License	Repo使用非准入的 License	定义的可引入 license 合集	提取PR合入目标代码的Repo级License、增量文件的License清单，分析**License是否准入**	**SUCCESS**：Repo/PR增量代码的License符合License准入清单 **FAILED**：Repo/PR增量代码的License不符合License准入清单(非准入、未识别)	Repo全部使用经过 License准入清单认证的 License
Copyright	缺乏Repo级的Copyright 声明	1.在根目录或者 1 层子目录，包括但不限于以下文件：License, copyright, readme, notice 中的任何一个文件中包含 copyrights 字段描述。	获取PR合入目标代码，分析前两层子目录下**是否存在Copyright**声明	**SUCCESS**：Repo存在Copyright声明 **WARNING**：Repo缺失Copyright声明	Repo级的Copyright建议使用以下两种方式之一： a. 在根目录下放单独的 Copyright Notice 文件。 b.在 Notice 子目录下放单独的完整 Notice 文件。

- ✓ License准入清单：

  https://compliance.openeuler.org/license-list

- ✓ 24年1-6月合规门禁检查正确率：**97%**

```
2024-05-08 15:25:58,434 [   INFO] : check mysql license ...
2024-05-08 15:28:40,494 [   INFO] : the license in spec is free
2024-05-08 15:28:40,495 [   INFO] : check license_in_spec pass
2024-05-08 15:28:40,495 [WARNING] : the license in scope is not pass, notice: 存在非准入License: FreeBSD-DOC(mysql/mysql-8.0.35/LICEN
2024-05-08 15:28:40,495 [  ERROR] : check license_in_src fail
2024-05-08 15:28:40,496 [   INFO] : all licenses from src:
2024-05-08 15:28:40,496 [   INFO] : licenses in src:set() and in spec:GPLv2 with exceptions and LGPLv2 and BSD-2-Clause are same
2024-05-08 15:28:40,496 [   INFO] : check license_is_same pass
2024-05-08 15:28:40,497 [   INFO] : the copyright in repo is pass
2024-05-08 15:28:40,497 [   INFO] : check copyright_in_repo pass
```

License门禁问题

- **Spec文件包含多License场景时，只对第一个license检查；**

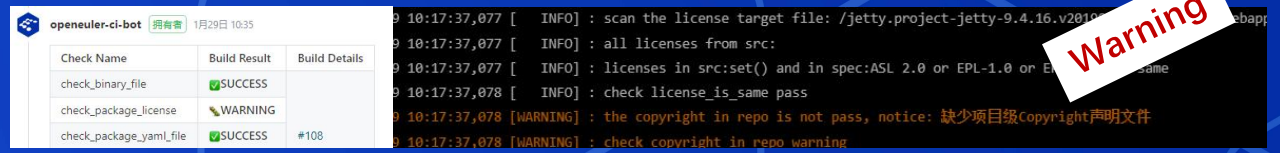
  不能有效拦截子包license问题；

  https://gitee.com/src-openeuler/jetty/pulls/71

  https://openeulerjenkins.osinfra.cn/job/multiarch/job/src-openeuler/job/trigger/job/jetty/108/console

  ——表现：license检查缺失copyright评论报warning，标签未呈现ci_failed；

  ——风险：版本发布软件包的license存在风险；

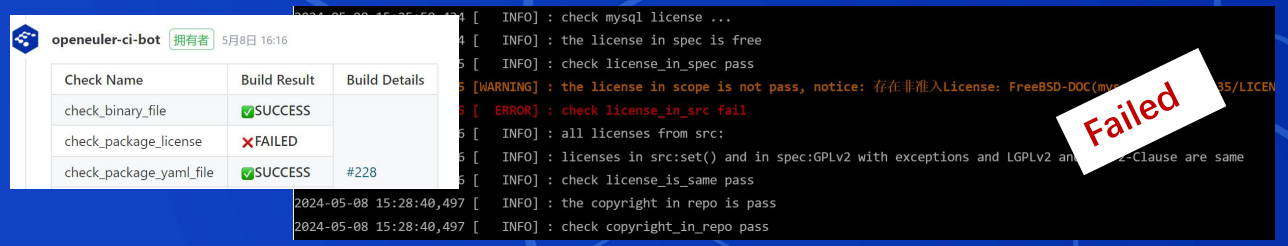


- **License检查结果未在门禁结果中呈现；**

  https://gitee.com/src-openeuler/mysql/pulls/133

  ——表现：license未准入检查失败，评论**FAILED**，标签未呈现ci_failed；

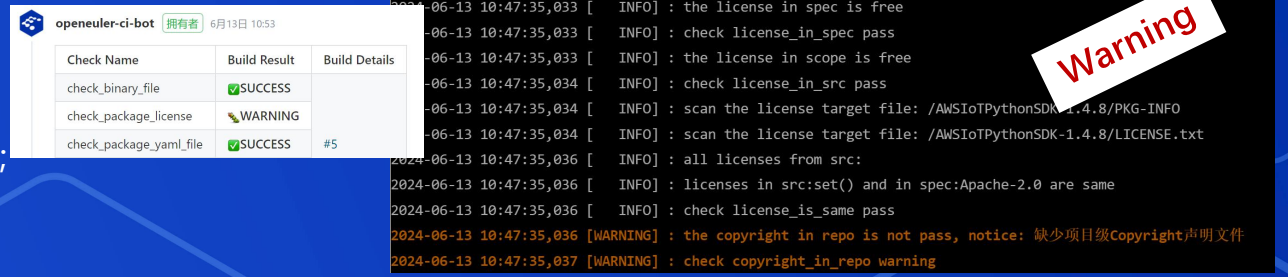
  ——风险：软件包license出现不合规风险；



  https://gitee.com/src-openeuler/python-AWSIoTPythonSDK/pulls/6

  ——表现：检查出copyright缺失， 评论**WARNING**，标签未呈现ci_failed；

  ——风险：软件包license出现不合规风险；



  ——风险：软件包license出现不合规风险；

- **门禁检查日志呈现上不方便查看；**

  比如License检查结果在日志中不容易被发现； License准入清单在门禁评论区和日志中未呈现；

版本问题

- **openEuler版本中安全扫描检查出5.8k（40.7k）不符合license准入列表要求的二进制包license**

  ✓ 问题一：license检查结果为NOT_ALLOW，license准入列表中存在此license，但是license的版本不准入

  https://compliance.openeuler.org/check?license=PHP

  解决方案：~~license的版本进行整改通过~~，对于特殊文件的license给出说明或者评审（如：Verbatim是违规的，但是使用 Verbatim license的都是linux手册，在特殊情况的适用范围内。）

  ✓ 问题二：license检查结果为UNKNOWN，license准入列表中不存在此license或存在不规范连接词，检查不出是否合规

  https://compliance.openeuler.org/check?license=Apache License, Version 2.0

  解决方案：license连接词不规范，修改连接词；license信息在license准入列表中不存在，对其进行评审，评审过后将其新增到license准入列表中，或者直，接将其更改为ALLOW的license

优化方案

- **Spec文件存在多license场景时，需要在门禁检查中识别处理；——合规**
- **针对软件包扫描发现的UNKNOW的license（267个）进行评审；——合规**
- **License检查中一致性检查从旧方案迁移到合规统一处理；——门禁&合规**
- **求助社区openDesign SIG优化门禁呈现的体验；——openDesign&门禁**
  - 接口变更检查清单 新增说明，描述问题内涵和处理方法；
  - @PR提交人和门禁后置处理事项提醒 放在一个评论中完成；

决策项

- **门禁检查失败项是否作为 代码合入 强制控制点?**
  - 若是，哪些项目作为强制确认项?
- **License检查是否需要影响门禁检查结果？（CI标签）**
- **其他静态检查项是否影响门禁检查结果？（CI标签）**
- **24.03_LTS & 22.03_LTS_SP4版本的license合规问题是否遗留，持续整改，下版本前完成?**

THANKS

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler