

PR #21423 完整报告

sgl-project/sglang

[AMD] Fix AMD CI: mark /sglang-checkout as git safe.directory in container

合并时间: 2026-03-26 10:18

原文链接: <http://prhub.com.cn/sgl-project/sglang/pull/21423>

执行摘要

本 PR 修复了 AMD CI 工作流中因 git 所有权检查失败导致的依赖安装错误，通过添加 git 安全目录配置确保容器内 root 用户可访问代码目录，恢复所有 AMD CI 正常运行。

功能与动机

由于 `setuptools-scm` 更新至 v9+ 后，将 git 的“dubious ownership”错误视为致命，而 CI 容器以 root 用户运行，代码检出属于非 root 的 runner 用户，导致 git 拒绝访问，从而使所有 AMD CI 工作流（如 Nightly Test 和 PR Test）从 2024 年 3 月 25 日开始在“Install dependencies”阶段失败。此 PR 旨在快速修复此回归问题，避免影响团队开发和测试流程。

实现拆解

关键改动在两个 AMD CI 启动脚本中：

- `scripts/ci/amd/amd_ci_start_container.sh` 和 `scripts/ci/amd/amd_ci_start_container_disagg.sh` 均在容器启动命令后添加一行：`bash docker exec ci_sglang git config --global --add safe.directory /sglang-checkout` 该命令将 `/sglang-checkout` 目录标记为 git 安全目录，允许跨用户访问，解决 `setuptools-scm` 版本内省时的所有权错误。

评论区精华

review 中没有实质性讨论，只有两位 reviewer（bingxche 和 yctseng0211）批准，表明变更直接且被团队接受，无设计争议或技术辩论。

风险与影响

- 风险：更改仅涉及 git 全局配置，风险较低；但需注意在复杂多容器环境中可能干扰其他 git 操作，不过已验证通过 CI 测试，回归风险小。
- 影响：修复了所有 AMD CI 工作流，使依赖安装阶段恢复正常，对用户和系统其他部分无直接影响，仅提升 CI 基础设施的稳定性和团队开发效率。

关联脉络

从近期历史 PR 看，此 PR 是团队持续优化 CI 基础设施的一部分：

- PR #21338 修复 CI 资源泄漏，强调环境问题处理。
- PR #21345 改进 CI 性能，减少速率限制消耗。

- PR #21428 修复 AMD 平台启动崩溃，凸显该平台的特殊性。这些 PR 共同反映团队对 CI 稳定性和跨平台支持的重视，本 PR 作为快速响应外部依赖变化的案例，值得在类似调试场景中参考。