PR #24265 完整报告

sgl-project/sglang

[CI] drop --prerelease allow from uv pip install suffix

合并时间：2026-05-03 03:25

原文链接：http://prhub.com.cn/sgl-project/sglang/pull/24265

执行摘要

- 一句话：删除 --prerelease allow 以提升 CI 稳定性
- 推荐动作：该 PR 变更简单明确，可作为 CI 最佳实践的参考：显式禁止预发布版本可避免意外引入不稳定的依赖。建议同时评估是否移除 unsafe-best-match 以增强安全性。

功能与动机

apache-tvm-ffi 0.1.11rc2 预发布版本因 build_inline() 中的 FileNotFoundError 导致 CI 崩溃。虽然最终发现根本原因是容器挂载缓存问题，但删除 --prerelease allow 可避免未来类似预发布版本意外引入。

实现拆解

1. 修改 scripts/ci/cuda/ci_install_dependency.sh 中的 PIP_INSTALL_SUFFIX 变量，去掉 --prerelease allow 参数。
2. 最初同时添加了 apache-tvm-ffi < 0.1.11 版本上限，但后续回滚，仅保留标志删除。

关键文件：

- scripts/ci/cuda/ci_install_dependency.sh（模块 CI 脚本；类别 infra；类型 infrastructure）：核心变更文件，修改了 PIP_INSTALL_SUFFIX 标志

关键符号：未识别

评论区精华

gemini-code-assist[bot] 在 review 中提出应同时移除 --index-strategy unsafe-best-match 标志，因为它可能导致依赖混淆攻击。但该建议未在 PR 中被采纳。

- 不建议使用 unsafe-best-match 标志 (security): 未被采纳，仅移除了 --prerelease allow

风险与影响

- 风险：直接风险极低：仅更改 CI 依赖安装时的版本选择策略，不影响运行时逻辑。间接风险：若某个依赖的稳定版本存在 bug，而预发布版本包含修复，则删除该标志可能导致 CI 错过修复版本。

- 影响：影响范围：仅限 CI 环境，对所有 CI 流水线的依赖安装步骤生效。影响程度：低，因为 CI 原本已在生产环境中使用 --prerelease allow，删除后会使版本选择更保守。
- 风险标记：低风险变更，依赖版本策略调整

关联脉络

- PR #21247 [Dependency] Upgrade to Torch 2.11.0: 同属依赖管理变更，涉及 CI 依赖安装