PR #35750 完整报告

sgl-project/sglang

[CI] Gate `/rerun-test` on commenter trust and remove `/rerun-stage`

合并时间：2026-08-21 06:05

原文链接：http://prhub.com.cn/sgl-project/sglang/pull/35750

执行摘要

- 一句话：移除 /rerun-stage，重跑命令按评论者信任门控
- 推荐动作：值得精读，特别是权限模型简化与安全加固设计。关注点：cooldown_interval_minutes 复用为信任标记，以及 rerun-test.yml 中显式声明 permissions 的写法。若参与 CI 治理，可借鉴其以最少配置表达信任级别的思路。

功能与动机

PR body 指出 /rerun-stage 命令只发布弃用提示，阶段级调度仍可通过 Actions UI 使用，因此可移除；而选择性重跑分发 rerun-test.yml 不经过 pr-gate.yml，不受限流，现有的 cooldown_interval_minutes 和写权限正是 pr-gate.yml 的豁免信号，所以直接用这两个信号作为门控，避免引入新权限键。同时修复了 checkout 在 .git/config 中残留作业令牌的安全隐患。

实现拆解

1. 移除 /rerun-stage 命令：在 scripts/ci/utils/slash_command_handler.py 中删除相应分支，在 .github/workflows/slash-command-handler.yml 中移除 contains() 触发条件，并从 .github/CI_PERMISSIONS.json 全部 241 个条目中删除 can_rerun_stage 字段。
2. 重跑门控改造：重写 _check_rerun_test_permissions 函数，先检查 user_perms['cooldown_interval_minutes'] == 0 直接放行，否则通过 get_collaborator_permission 验证评论者是否有 admin/write 权限，均不满足时拒绝并回复提示。
3. 主流程调整：main() 中移除用户不在权限文件时立即退出的逻辑，使仅具写权限的用户也能进入门控；PR 作者仅保留 can_rerun_failed_ci，不再自动获得 can_rerun_test。
4. 工作流加固：在 rerun-test.yml 的三个 checkout 中添加 persist-credentials: false，并移除工作流级 actions: write 权限块，避免 fork 代码读取作业令牌。
5. 文档同步：更新 .github/FOLDER_README.md、contribution_guide.mdx、test/README.md 及 AMD workflow 注释，修正 fork 作者权限表述并移除 /rerun-stage 引用。

关键文件：

- .github/CI_PERMISSIONS.json（模块 CI 权限；类别 infra；类型 permission-config）：核心配置变更，所有 241 个权限条目移除 can_rerun_stage 键，直接体现权限模型简化。

- scripts/ci/utils/slash_command_handler.py（模块 命令处理；类别 infra；类型 core-logic；符号 _check_rerun_test_permissions, main）：重跑命令的门控逻辑在此改写，是行为变化的核心实现。
- .github/workflows/rerun-test.yml（模块 重跑工作流；类别 infra；类型 infrastructure）：安全加固关键点：为 PR 分支 checkout 禁用凭据持久化，并移除无效的工作流级写权限。
- .github/update_ci_permission.py（模块 权限生成器；类别 infra；类型 infrastructure；符号 main）：权限生成模板同步更新，确保未来生成的权限文件不再包含 can_rerun_stage。
- .github/FOLDER_README.md（模块 仓库文档；类别 docs；类型 documentation）：记录权限键与冷却时间 / 重跑耦合的说明，便于维护者理解新的权限语义。

关键符号：_check_rerun_test_permissions, main, main

关键源码片段

scripts/ci/utils/slash_command_handler.py

重跑命令的门控逻辑在此改写，是行为变化的核心实现。

```
def _check_rerun_test_permissions(gh_repo, pr, comment, user_perms, command_name):
    # 重跑命令不经过 pr-gate.yml，因此不受速率限制；
    # 门控标准与 pr-gate.yml 的豁免信号保持一致：零冷却时间或仓库写权限。
    if user_perms.get("cooldown_interval_minutes") == 0:
        # 零冷却时间意味着完全信任，直接放行，避免额外 API 调用。
        return True

    commenter = comment.user.login
    perm = gh_repo.get_collaborator_permission(commenter)
    if perm in ("admin", "write"):
        # 写权限以上协作者无论 PR 来源均可重跑。
        print(f"Commenter {commenter} has write+ permission. Proceeding.")
        return True

    # 其余情况一律拒绝，并给评论者明确反馈。
    print(f"Permission denied: /{command_name} by {commenter} (permission: {perm}).")
    comment.create_reaction("confused")
    pr.create_issue_comment(
        f"😕 `/{command_name}` requires `cooldown_interval_minutes: 0` in "
        "`.github/CI_PERMISSIONS.json`, or write permission on the repo.

"
        "Please ask a maintainer to run this command, or use the normal CI flow."
    )
    return False
```

.github/workflows/rerun-test.yml

安全加固关键点：为 PR 分支 checkout 禁用凭据持久化，并移除无效的工作流级写权限。

```
jobs:
```

```
rerun_test:
  runs-on: [self-hosted, gpu]
  permissions:
    contents: read
    issues: read
    # 每个作业自行声明 permissions，替换而不是合并工作流级块；
    # 不声明 actions: write，防止作业获得不必要的写令牌。
  steps:
    - uses: actions/checkout@v4
      with:
        ref: ${{ inputs.pr_head_sha || github.sha }}
        # 该 checkout 可能包含 fork 的代码，会被后续步骤执行；
        # 不设置 persist-credentials，防止作业令牌残留在 .git/config 中被读取。
        persist-credentials: false
```

评论区精华

无 review 评论。PR body 中详细阐述了设计决策：不新增权限键，用现有 cooldown 值承担信任级别；选择性重跑不受限流；作者身份不授予重跑权限。

- 暂无高价值评论线程

风险与影响

- 风险：权限模型变更可能导致 67 个拥有非零冷却时间的 custom override 账号失去选择性重跑能力，需与贡献者协调；.github/CI_PERMISSIONS.json 全量修改与 #35600 必然冲突；移除 /rerun-stage 可能影响依赖该命令的外部脚本；安全问题主要集中在 rerun-test.yml 中 checkout 的凭据处理，persist-credentials: false 依赖 GitHub Actions 语义。
- 影响：影响所有 CI 贡献者：174 人保留访问（151 人通过冷却时间 0，23 人通过写权限），67 人失去，16 人新增。对团队而言简化了权限维护，统一了门控逻辑；对系统安全而言修复了高风险的令牌泄漏路径。不影响运行时功能与性能。
- 风险标记：权限范围变更影响 67 个账号，配置文件全量修改易致冲突，已移除命令可能被外部流程依赖，安全加固依赖 checkout 行为

关联脉络

- PR #35600 Add CI permissions for four contributors: 两个 PR 都修改 .github/CI_PERMISSIONS.json 的全部条目，且 PR body 明确提及冲突关系。