PR #2403 完整报告

radixark/miles

fix(ci): unblock ROCm fork PRs at checkout

合并时间：2026-08-12 13:45

原文链接：http://prhub.com.cn/radixark/miles/pull/2403

执行摘要

- 一句话：ROCm fork PR 改走低信任 pull_request，修复 checkout 失败
- 推荐动作：值得精读。该 PR 展示了 GitHub Actions 信任模型变更下的最佳实践：不要用 allow-unsafe-pr-checkout 绕过守卫，而是迁移到 pull_request 低信任事件，让 secrets 保护与 merge commit 检出由平台接管。同时可参照其测试策略（用字符串断言锁定 workflow 的关键属性）来防控类似 CI 回归。

功能与动机

在 PR #2347 中，带有 run-ci-amd 标签的 fork PR 在 actions/checkout 阶段即失败，报错 Refusing to check out fork pull request code from a 'pull_request_target' workflow。根因是 pr-test-rocm.yml 使用 pull_request_target 事件并从 fork 显式 checkout refs/pull//merge，而 actions/checkout 在 2026-07-20 新增守卫后拒绝对 fork 代码在可信上下文中检出。本 PR 将 ROCm 工作流迁移到与 NVIDIA 工作流一致的 pull_request 低信任模型，让 checkout 默认选择 PR merge commit，并移除 target-only 授权输出与不安全开关。

实现拆解

1. 触发事件切换：.github/workflows/pr-test-rocm.yml 中 on.pull_request_target 改为 on.pull_request，resolve-ci-policy 的 EVENT_NAME 直接使用 github.event_name，并删除 Authorize self-hosted PR execution 步骤及 allow_self_hosted 输出。
2. stage 门禁简化：stage-c-4-gpu-mi300x 删除 if: needs.resolve-ci-policy.outputs.allow_self_hosted == 'true'，不再传 checkout_ref；WANDB_API_KEY 从条件表达式改为 ${{ secrets.WANDB_API_KEY }}，由 GitHub 对 fork 自动隐藏。
3. 可复用工作流收敛：.github/workflows/_run-ci-rocm.yml 删除 checkout_ref 输入定义及 checkout 步骤的 ref，让 actions/checkout@v4 默认解析 PR merge commit，保留 persist-credentials: false。
4. 测试与文档同步：tests/ci/test/test_run_suite.py 的 TestRocmWorkflowScopeSeam 断言改为验证 pull_request 事件、禁止 pull_request_target、确认 allow_self_hosted 与 checkout_ref 消失；docs/ci/00-stage.md 更新信任模型说明。
5. 验证：pytest tests/ci/test/test_run_suite.py -k RocmWorkflowScopeSeam 通过 2 项，pre-commit run check-yaml 通过。

关键文件：

- .github/workflows/pr-test-rocm.yml（模块 CI 工作流；类别 infra；类型 infrastructure）：核心变更：触发事件从 pull_request_target 改为 pull_request，移除 authorize 授权步骤与显式 checkout_ref，是该修复的主战场。
- .github/workflows/_run-ci-rocm.yml（模块 复用工作流；类别 infra；类型 infrastructure）：可复用工作流删除 checkout_ref 输入与显式 ref，让默认 checkout 解析 PR merge commit。
- tests/ci/test/test_run_suite.py（模块 测试套件；类别 test；类型 test-coverage）：测试配套更新，锁定新的工作流信任模型，防止回归。
- docs/ci/00-stage.md（模块 CI 文档；类别 docs；类型 documentation）：同步更新 CI 文档中的信任模型与 secrets 说明，帮助维护者理解新行为。

关键符号：test_pr_nightly_and_dispatch_share_policy, test_stage_consumes_policy_and_preserves_manual_full_scope

关键源码片段

tests/ci/test/test_run_suite.py

测试配套更新，锁定新的工作流信任模型，防止回归。

```
class TestRocmWorkflowScopeSeam:
    @staticmethod
    def _workflow() -> str:
        return (Path(__file__).resolve().parents[3]
                / '.github' / 'workflows' / 'pr-test-rocm.yml').read_text()

    def test_pr_nightly_and_dispatch_share_policy(self):
        workflow = self._workflow()
        # pull_request 事件必须存在，且不允许残留 pull_request_target
        assert 'pull_request:' in workflow
        assert 'pull_request_target:' not in workflow
        policy_block = workflow.split('resolve-ci-policy:', 1)[1].split('resolve-ci-image:', 1)[0]
        # 自建授权步骤已移除，allow_self_hosted 门禁不再存在
        assert 'allow_self_hosted' not in policy_block
        assert 'EVENT_NAME: ${{ github.event_name }}' in policy_block

    def test_stage_consumes_policy_and_preserves_manual_full_scope(self):
        workflow = self._workflow()
        stage = workflow.split('  stage-c-4-gpu-mi300x:', 1)[1]
        command = stage.split('execute_command:', 1)[1].split('secrets:', 1)[0]
        assert 'needs: [resolve-ci-policy, resolve-ci-image]' in stage
        assert 'allow_self_hosted' not in stage
        assert 'checkout_ref:' not in stage
        assert 'WANDB_API_KEY: ${{ secrets.WANDB_API_KEY }}' in stage
        reusable = (Path(__file__).resolve().parents[3]
                    / '.github' / 'workflows' / '_run-ci-rocm.yml').read_text()
        assert 'checkout_ref:' not in reusable
```

```
assert 'persist-credentials: false' in reusable
assert 'allow-unsafe-pr-checkout' not in reusable
```

评论区精华

仓库内无独立 review 评论，但提交历史揭示了方案迭代：首个提交 e6de779 选择在 checkout 中显式设置 allow-unsafe-pr-checkout 快速解封；最终提交 6e331ac 则完全改用 pull_request 低信任事件模型，与 NVIDIA 的 pr-test.yml 保持一致，并删除授权步骤与会话开关。reviewer guapisolo 直接批准最终方案，且最终提交由 guapisolo 本人完成重写，说明团队更倾向于避免使用不安全开关、统一信任边界。

- 修复方案：allow-unsafe-pr-checkout 还是 pull_request 模型？ (design): 采用 pull_request 事件 + 默认 merge commit checkout，由 GitHub 统一管理 fork 的 secrets 隐藏。

风险与影响

- 风险： 1) 自托管 runner 暴露面未变：fork PR 代码在获得标签后仍会在 MI300X 自托管 runner 上执行，依赖维护者加标签的审批流程； 2) secrets 处理依赖 GitHub 保证：WANDB_API_KEY 直接引用 secrets，fork 运行会被 GitHub 置空，若测试逻辑假设 key 存在可能产生行为差异，但不会泄漏； 3) 事件字段兼容性：pull_request 与 pull_request_target 的 github.event.pull_request 结构一致，github.event.schedule 仅用于 schedule 触发，workflow_dispatch 分支保持原样，回归风险低； 4) 文档与测试同步，未引入新的部署配置。
  - 影响：对 fork 贡献者：ROCm 相关 PR 不再因 checkout 拒绝而阻塞，只要维护者打上 run-ci-amd 等标签即可在 MI300X 上运行测试；对维护者：CI 安全模型与 NVIDIA 工作流统一，减少自建授权步骤，降低维护成本；对系统：pr-test-rocm.yml 事件触发语义变化，今后无法在 pull_request_target 可信上下文中使用仓库 secrets，但当前阶段不需要。整体影响范围限于 CI 基础设施与 AMD/ROCm 测试路径。
  - 风险标记：安全模型变更，自托管 runner 暴露，secrets 依赖平台保证

关联脉络

- PR #2265 [AMD] 在 ROCm 上启用 Qwen3 FSDP 混合分片 CI: 同为 AMD/ROCm 的 CI 修复，围绕 MI300X 自托管 runner 的 CI 能力，与本 PR 的 ROCm 测试工作流直接相关。
- PR #2404 安装 kubernetes 工具链、charts 和 k8s provider 所需依赖：同属 CI 基础设施演进，预装 k8s 工具链与本次工作流信任模型调整共同完善 CI 基础环境。