

PR #2233 完整报告

radixark/miles

examples: rename swe-agent to swe-agent-harbor-docker

合并时间: 2026-08-07 06:00

原文链接: <http://prhub.com.cn/radixark/miles/pull/2233>

执行摘要

- 一句话: 重命名 swe-agent 示例为 swe-agent-harbor-docker, 明确沙箱后端
- 推荐动作: 值得快速阅读, 作为“目录重命名如何安全落地”的样板: git 重命名保留历史、受限替换代替全局 find-replace、静态路径审计作为无 CI 覆盖时的验证手段。不建议作为核心逻辑精读, 因为不含任何行为级变更。

功能与动机

examples 下同时存在 swe-agent 与 swe-agent-harbor-daytona 两个 Harbor 配方, 唯一区别是任务沙箱运行在本地 Docker 还是 Daytona 云沙箱, 但目录名只体现了一个后端。PR body 原话: Someone scanning the directory listing cannot tell that the first is the Docker-backed sibling of the second rather than an unrelated pipeline, 导致 Daytona README 需要专门在开头解释两者关系。重命名让“沙箱后端”成为两个目录的共同命名轴。对于 URL slug 疑虑, 作者核查 docs/docs.json 无 swe-agent 页面, Mintlify 导航不受目录移动影响, 仅需更新 github 链接。

实现拆解

1. 目录迁移与重命名: 将 examples/swe-agent 下 6 个文件整体 mv 至 examples/swe-agent-harbor-docker。其中 download_and_process_data.py、generate.py、run-glm47-flash-agent-async.py、run.py、swe_agent_function.py 为字节级零改动, git 识别 100% 相似; README.md 改动 4 行 (标题加入 Docker sandboxes, 命令路径同步)。这样目录对与 swe-agent-harbor-daytona 对称, README 不再需要在开头解释兄弟关系。
2. 受限路径替换 (guarded sweep): 在 examples/README.md、examples/experimental/swe-agent-harbor-daytona/README.md、launch_agent_server.sh、docs/user-guide/rollout-endpoints.md、docs/user-guide/harbor.md、docs/user-guide/agent-ic-chat-template.md、examples/experimental/openenv/openenv_generate.py 等处更新 examples/swe-agent -> examples/swe-agent-harbor-docker 的路径引用。刻意不做全局 find-replace, 因为 mini-swe-agent / mini_swe_agent_2 harness 与目录名共享 sub-string, 批量替换会误伤使用它们的 9 个文件。
3. 文档路由核验: 检查 docs/docs.json 无 swe-agent 页面, 确认 Mintlify 路由不受目录移动影响; 受影响的外部公开 URL 仅为 docs/user-guide 内的 github tree/blob 链接, 已逐

一更新。

4. 静态审计（替代 CI 测试）：examples 位于 pytest 的 norecursedirs 中，CI 无法 import 示例代码，因此采用四项静态核验：所有 tracked files 中的 examples/ token 均可解析，14 个失败 token 与父 commit 完全一致（零新增回归）；无 dotted examples.swe 引用；无 from examples.swe import；mini-swe-agent / mini_swe_agent_2 全部保持原样；同时 black/isort/py_compile 通过。
5. 配套与验证边界：未启动任何训练端到端验证，变更被声明为路径级、运行时无 launcher 解析该示例目录；无新增 CI 测试。

关键文件：

- examples/swe-agent-harbor-docker/README.md（模块 示例代码；类别 docs；类型 rename-or-move）：重命名后唯一有内容调整的文档：标题点明 Docker 沙箱后端，命令路径同步到新目录，是全 PR 对读者最直接的入口。
- examples/experimental/openenv/openenv_generate.py（模块 沙箱编排；类别 source；类型 reference-update）：源码文件中唯一被修改的入口：虽然只改 docstring 引用，但它是 openenv/tbench2 与 swe-agent 示例 reward 函数镜像关系的记录点。
- examples/experimental/swe-agent-harbor-daytona/README.md（模块 实验示例；类别 docs；类型 documentation）：Daytona 配方的 README 是重命名的主要受益者：不再需要在开场长段解释与 swe-agent 的关系，直接引用新目录名即可。
- examples/swe-agent-harbor-docker/run.py（模块 示例代码；类别 infra；类型 rename-or-move）：训练启动器入口，字节级重命名后所有文档示例命令都指向新路径。
- examples/swe-agent-harbor-docker/download_and_process_data.py（模块 示例代码；类别 infra；类型 rename-or-move）：数据转换脚本，因 README 与 launcher 引用同步迁移而一并重命名。
- examples/swe-agent-harbor-docker/generate.py（模块 示例代码；类别 infra；类型 rename-or-move）：reward 函数入口，与 openenv_generate.py 的 docstring 引用形成对应关系。
- examples/swe-agent-harbor-docker/run-glm47-flash-agentic-async.py（模块 示例代码；类别 infra；类型 rename-or-move）：GLM-4.7-Flash 的 agentic async 启动脚本，随目录整体移动。
- examples/swe-agent-harbor-docker/swe_agent_function.py（模块 示例代码；类别 infra；类型 rename-or-move）：agent 函数实现，docs/user-guide/rollout-endpoints.md 中 abort 参考链接指向该文件的新路径。
- examples/experimental/swe-agent-harbor-daytona/launch_agent_server.sh（模块 实验示例；类别 other；类型 reference-update）：Daytona agent server 启动脚本注释中的 launcher 路径同步更新，避免引导用户跳到旧目录。
- docs/user-guide/rollout-endpoints.md（模块 用户文档；类别 docs；类型 documentation）：用户文档核心入口之一，更新环境变量提示、示例链接与 abort 参考链接，是文档侧改动量最大的文件。
- docs/user-guide/harbor.md（模块 用户文档；类别 docs；类型 documentation）：Harbor 相关用户文档，路径引用同步到新目录。

- examples/README.md (模块 示例代码; 类别 docs; 类型 documentation) : examples 目录总览, 更新 swe-agent 条目路径, 避免读者进入 404。
- docs/user-guide/agentic-chat-template.md (模块 用户文档; 类别 docs; 类型 documentation) : agentic chat template 文档中的示例路径引用同步更新。

关键符号: 未识别

关键源码片段

examples/swe-agent-harbor-docker/README.md

重命名后唯一有内容调整的文档: 标题点明 Docker 沙箱后端, 命令路径同步到新目录, 是全 PR 对读者最直接的入口。

```
# 标题: SWE-Agent training with Harbor on Docker sandboxes
# 标题加入 Docker sandboxes, 与 examples/experimental/swe-agent-harbor-daytona
# 形成对称命名;
# 下方命令路径全部从 examples/swe-agent 迁移到 examples/swe-agent-harbor-docker。
python examples/swe-agent-harbor-docker/run.py ... --extra-env-vars 'AGENT_TRIAL_TIMEOUT=
10800'
python examples/swe-agent-harbor-docker/download_and_process_data.py \
--input /path/to/terminal-bench.jsonl \
--output /path/to/tb2_train.jsonl \
--agent-name mini-swe-agent
```

examples/experimental/openenv/openenv_generate.py

源码文件中唯一被修改的入口: 虽然只改 docstring 引用, 但它是 openenv/tbench2 与 swe-agent 示例 reward 函数镜像关系的记录点。

```
"""Reward function for the OpenEnv Terminal-Bench-2 (tbench2) run.
```

```
Task-agnostic: the agent function (``openenv_agent_function.run``) stores the
env-computed binary pytest reward in ``sample.metadata["reward"]``; this just
reads it back. Wired via ``--custom-rm-path openenv_generate.reward_func`` and
mirrors ``swe-agent-harbor-docker/generate.py:reward_func`` so it works for both the
single-sample (``async_rm``) and batched (``--custom-rm-path``) call paths.
```

```
"""
```

```
from miles.utils.types import Sample
```

```
async def reward_func(args, samples: Sample | list[Sample], **kwargs) -> float | list[float]:
```

```
# 本 PR 唯一改动: docstring 中的路径从 swe-agent/generate.py 更新为
# swe-agent-harbor-docker/generate.py, 使两个示例入口的镜像关系在新目录布局下
# 仍然可追溯; 函数体本身未做任何变更。
if isinstance(samples, list):
    return [s.metadata.get("reward", 0.0) for s in samples]
return samples.metadata.get("reward", 0.0)
```

评论区精华

本 PR 内 0 条 review 评论，nblintao 直接 APPROVED（空 body）。实质讨论发生在被堆叠的 #1919 / #2228：nblintao 在 #1919 中提问是否应把 swe-agent 重命名为 swe-agent-harbor-docker 或保留 url slug；#2228 的 review 推动去掉 ../swe-agent 相对引用、统一从仓库根路径引用 sibling 文件；由于 #2228 在 examples/swe-agent/ 内修改了两个文件，本 PR 特意先合并 #2228 再重命名目录以避免冲突。PR 内没有未解决的 open concerns。

- 是否重命名 swe-agent 为 swe-agent-harbor-docker (design): 重命名目录为 swe-agent-harbor-docker，旧路径不再保留，所有内部链接已同步更新。
- 防止误改 mini-swe-agent / mini_swe_agent_2 子串 (correctness): 采用受限替换（guarded sweep），并静态核验所有 mini-swe-agent / mini_swe_agent_2 出现均保持原样。
- 静态路径审计代替 CI 测试 (testing): 路径审计通过，PR 合并时无需新增 CI 用例；回归防护依赖后续 review 与手工核验。

风险与影响

- 风险：主要风险集中在引用断裂与覆盖度。
- 外部引用断裂：docs/user-guide 和 examples/README 中指向 github.com/.../examples/swe-agent 的链接若不更新会 404，本 PR 已全部更新，但仓库外的个人脚本、博客与 fork 若继续使用旧路径将失效。
- 静态路径审计未固化进 CI：后续新增对旧路径的引用不会自动失败，只能靠 review 复查；且 14 个既存失败 token 依旧存在（与父 commit 相同），本 PR 未修复也未新增。
- 无端到端测试：训练未实际运行，若存在运行时解析示例目录的 launcher（作者判断没有），可能漏检。
- mini-swe-agent 子串守卫：若后续有人做全局 renaming，会误伤 mini-swe-agent / mini_swe_agent_2 harness，属于需要持续留意的维护约定。
- 对核心训练代码零影响：miles/ 下无任何改动。
- 影响：影响面限于示例目录与文档：用户运行 swe-agent Docker 配方必须改用 examples/swe-agent-harbor-docker 路径；文档中的 github 链接已更新；examples 目录现在两个 Harbor 配方命名对称。对系统、训练管线、CI 均无运行影响；examples 不在 CI import 范围，docs/docs.json 无路由变化。团队后续新增 sandbox 后端时命名约定更清晰；短中期对外文档和草稿可能残留旧路径。
- 风险标记：旧路径外部引用断裂风险，静态路径审计未纳入 CI，无端到端训练验证，mini-swe-agent 子串需持续守卫

关联脉络

- PR #2228 examples: add swe-agent-harbor-daytona（标题据 commit message 归纳）：本 PR 直接栈于 #2228；#2228 在 examples/swe-agent/ 内修改了两个文件，若并行分支直接重命名目录会冲突，因此先合并 #2228 再重命名。

- PR #1919 swe-agent Harbor 示例系列 (PR body 引用) : nblintao 在该 PR 提问是否应把 swe-agent 重命名为 swe-agent-harbor-docker; 本 PR 直接回答该问题。
- PR #1818 移除 --tito-allowed-append-roles (commit message 引用) : commit 12e7742 说明 #1818 移除了该 flag, 导致 Daytona 示例无法保留独立 launcher, 转而复用 examples/swe-agent/run.py; 这使重命名后的目录可读性更加重要。