

PR #2863 完整报告

radixark/miles

openenv tb2 recipe: pin mcp below 2 in the server layer

合并时间: 2026-09-02 23:15

原文链接: <http://prhub.com.cn/radixark/miles/pull/2863>

执行摘要

- 一句话: 在 TB2 环境构建配方中锁定 `mcp<2`, 修复因 `mcp 2.0` 破坏性变更导致的 Camel-AI 导入失败。
- 推荐动作: 这是一个 值得精读但逻辑简单的bugfix PR。其价值不在于复杂的代码变更, 而在于清晰展示了对外部依赖破坏性变更的快速响应和修复模式 (在构建层通过版本约束进行缓冲)。对于维护依赖复杂生态系统的工程师来说, 此 PR 中详细的注释和提交说明是很好的实践范例。建议关注点在于其对依赖管理的处理方式, 以及如何通过注释和配方变更来隔离上游破坏性变更的影响。

功能与动机

为解决新构建的 `tbench2` 环境镜像 (TB2 images) 启动后每个 episode 都失败的根本问题。具体表现为 `ImportError: cannot import name 'FastMCP' from 'mcp.server'`。PR body 解释了根本原因: “camel-ai constrains only `mcp>=1.3`, and `mcp 2.0` (2026-07-28) dropped that re-export...”。解决方案是在服务器层安装依赖时主动锁定 `mcp` 版本。

实现拆解

1. 变更入口: 修改 `examples/experimental/openenv/tb2_sandbox_recipe.py` 文件中的 `server_layer_commands` 函数。该函数定义了构建任务环境服务器层的 shell 命令列表。
2. 核心逻辑调整: 在命令列表中 `uv pip install` 依赖安装的那一行, 追加了 '`mcp<2`' 约束。原命令为 `uv pip install ... /opt/src/tbench2_env_src uvicorn gradio`, 现改为 `uv pip install ... /opt/src/tbench2_env_src uvicorn gradio 'mcp<2'`。
3. 配套变更: 在修改的命令上方新增了 4 行注释, 详细说明了锁定 `mcp` 版本的原因 (camel-ai 依赖问题、`mcp 2.0` 的 breaking change) 以及此修复如何防止终端工具包导入失败。这确保了后续维护者能理解此特定版本锁定的意图。
4. 影响: 此变更仅影响通过此配方新构建的 TB2 服务器环境镜像。模板别名 (template alias) 会根据命令哈希变化触发重新构建, 因此已损坏的旧模板将不再被引用。

关键文件:

- `examples/experimental/openenv/tb2_sandbox_recipe.py` (模块 `OpenEnv` 配方; 类别 `source`; 类型 `configuration`; 符号 `server_layer_commands`): 这是定义 TB2 任务环境服务器层构建命令的核心配置文件。本次变更的唯一文件, 通过修改其中的 `pip install` 命令直接修复了环境构建失败的问题。

关键符号：server_layer_commands

关键源码片段

examples/experimental/openenv/tb2_sandbox_recipe.py

这是定义 TB2 任务环境服务器层构建命令的核心配置文件。本次变更的唯一文件，通过修改其中的 pip install 命令直接修复了环境构建失败的问题。

```
def server_layer_commands(task_dir: Path) -> list[str]:
    """The recipe itself: shell commands that turn the OFFICIAL task image
    into a combined task+env-server image. Nothing here is provider-specific —
    the same layers work for docker build, Daytona, Modal, ACA, etc.
    """
    return [
        # ... ( 前略, 安装系统包和 uv 的命令 )
        f"mkdir -p /opt/src && echo {_env_src_tar_b64()} | base64 -d | tar xz -C /opt/src",
        # mcp is pinned below 2: camel-ai constrains only mcp>=1.3, mcp 2.0
        # (2026-07-28) dropped the `from mcp.server import FastMCP` re-export
        # its TerminalToolkit imports, and every episode then fails with
        # "camel-ai (TerminalToolkit) is required for TB2".
        "/opt/uv/uv pip install --python /opt/envserver/bin/python /opt/src/tbench2_env_src uvicorn
        gradio 'mcp<2'",
        _task_layer_command(task_dir),
    ]

# ( 后略, 函数返回该列表 )
```

- 注释说明 *：此代码片段展示了 server_layer_commands 函数的核心部分。变更点在于 uv pip install 命令中新增的 'mcp<2' 约束。上方注释（由本次 PR 新增）清晰解释了锁定 mcp 版本的原因：camel-ai 的 TerminalToolkit 依赖 mcp 库中一个在 2.0 版本被移除的 FastMCP 导出。此修改确保了构建的环境服务器能正确导入该组件。

评论区精华

PR 评论区主要是自动化工具（[claude\[bot\]](#)）生成的评论和一位审核者（Shi-Dong）的快速批准（“LGTM!”）。未发现关于实现方案、风险或设计的实质性技术讨论。这表明变更本身非常直接，且修复意图清晰，获得了团队的迅速认可。

- 依赖版本锁定与兼容性修复 (design): 采用在服务器层安装命令中直接添加版本约束 ('mcp<2') 的方式被批准并合并。审核者（Shi-Dong）表示“LGTM!”。

风险与影响

- 风险：风险较低。主要风险是依赖版本锁定 (mcp<2) 可能在未来阻碍使用 mcp 库的 2.x 版本的新功能或安全更新。然而，当前 camel-ai 库对 mcp 的版本约束 (>=1.3) 尚未更新以兼容 2.x，因此此锁定是修复当前破坏性故障的必要临时措施。风险被评估为可控，因为影响范围仅限于 TB2 服务器环境镜像的构建层，不涉及核心训练或推理逻辑。

- 影响：影响范围明确且直接。直接影响的是 OpenEnv 集成中用于运行 tbench2 任务（TB2）的环境服务器镜像构建过程。修复后，新构建的镜像可以正常导入 Camel-AI 的 TerminalToolkit，从而使每个 episode 能够成功执行。对于用户（TB2 任务的测试者 / 开发者）而言，这意味着他们可以再次使用新环境进行评估和调试。对团队而言，确保了关键评估基础设施的正常运行。该修复不涉及 Miles 核心功能或 API 变更。
- 风险标记：依赖版本锁定

关联脉络

- PR #2811 openenv: raise the tbench2_env contract floor to OpenEnv#1025: 同为 OpenEnv 集成中关于 tbench2 环境的维护 PR，涉及相同的 key file (examples/experimental/openenv/openenv_launch_common.py)，共同维护 TB2 评估环境的稳定性。
- PR #2809 openenv e2b backend: declare the SDK as an extra, floor it at 2.12: 同为 OpenEnv 依赖管理 PR，处理另一个依赖（e2b SDK）的版本约束问题，共享 miles/rollout/agent/credentials.py 等文件。