

# PR #3213 完整报告

radixark/miles

docs: a page for setting a sandbox provider up, and one for adding a new one

合并时间: 2026-09-15 03:43

原文链接: <http://prhub.com.cn/radixark/miles/pull/3213>

## 执行摘要

- 一句话: 重组沙箱 provider 文档, 新增用户与开发者双页面
- 推荐动作: 值得快速浏览, 不必精读。本 PR 的借鉴价值在于信息架构决策: 按读者 (用户 vs 开发者) 切割文档、用“网格 + 勾选自带链接”表达跨模块兼容矩阵、以及“注册表条目即 provider 契约”的抽象。维护 agentic rollout 相关代码或文档的工程师, 应在后续 provider 相关 PR 中同步更新这两个新页面, 避免事实漂移。

## 功能与动机

PR body 明确说明动机: Provider setup (credential、endpoint、各 provider 的 quirks) 此前被复制进每个 recipe README 和 smoke 工具的 README, 而“how to add a provider”没有归属。因此按读者重新切割: 用户侧一页讲清每个 provider 怎么配, 开发者侧一页讲清新 provider 怎么接; 同时 environments.md 回归 connector 索引, recipe README 只保留与自身 launch 命令相关的一行, 其余链接到新页面。

## 实现拆解

1. 新增用户侧聚合页 [docs/user-guide/sandbox-providers.md](#) (+72)。页面核心是 provider x connector 网格: 行是 AgentENV、Daytona、E2B、Modal, 列是 Harbor、HUD、NeMo Gym、OpenEnv; 勾选表示该组合跑过真实 rollout, 列头链接到对应 connector 的 recipe, 小众组合 (如 AgentENV x OpenEnv、Daytona x Harbor) 的勾选自带独立链接。网格下方按 provider 给出凭据与端点配置: 统一契约是“环境变量或 key file 两种方式, launcher 只转发文件路径、不转发内容”, 并记录各 provider 怪癖——E2B Cloud 模板构建以非 root 用户进行、Daytona 有总磁盘配额、Modal 的 token pair 必须成对出现。
2. 新增开发者侧接入指南 [docs/developer/adding-a-sandbox-provider.md](#) (+45)。开篇立契约: “一个 provider 就是 [miles/rollout/agentic/credentials.py](#) 中 PROVIDER\_CREDENTIALS 的一个注册项, connector 代码不按 provider 分支”。四步流程: 注册表条目 → golden episode ([scripts/sandbox\\_smoke/run.py --connector harbor --backend <name>](#)) → GPU rollout ([HARBOR\\_ENV\\_TYPE=<name> + tests/e2e/agentic/test\\_harbor\\_rollout.py](#)) → 在网格中勾选并补配置小节。并用表格对照两个测试的分工: golden 测平台往返、rollout 测 harness + 会话服务器 + TITO 记录 + 奖励。

3. 去重与读者切割。[docs/user-guide/environments.md](#) 删除内嵌 provider 表，只留指向新页面的链接；[examples/experimental/openenv/README.md](#) 删除逐 provider 的凭据参数表，保留 provider 特有行为（模板预构建、agentenv 为 e2b 别名、e2b>=2.12 的版本约束注释），参数表里凭据行合并为一行指向新文档；[examples/experimental/harbor/README.md](#) 的 Validation 段从带日期 / 机型的运行记录压缩为一句“端到端跑过”，并把 --save-dir 磁盘空间警告保留在命令块之后；[scripts/sandbox\\_smoke/README.md](#) 删除“Exercised so far”运行记录表，因为实测组合记录已迁到用户侧网格。
4. 导航与引用一致性。[docs/docs.json](#) 把 [user-guide/sandbox-providers](#) 挂到 User Guide → Agentic Environments 分组、[developer/adding-a-sandbox-provider](#) 挂到 Developer Guide 顶层；[tests/e2e/agentic/test\\_harbor\\_rollout.py](#) 与 [test\\_sandbox\\_golden.py](#) 的 docstring 把“which combinations have been run”的引用从 [scripts/sandbox\\_smoke/README.md](#) 改为新文档表格，确保不会出现双份事实。
5. 配套。无源码、测试断言、配置或部署变更；纯文档与 docstring 引用更新，CI 行为不受影响。

关键文件：

- [docs/user-guide/sandbox-providers.md](#)（模块 用户文档；类别 docs；类型 documentation）：本 PR 核心新增页：provider × connector 实测网格 + 各 provider 凭据与端点配置指南，成为用户侧“单一事实来源”，替代散落在各 README 的重复说明。
- [docs/developer/adding-a-sandbox-provider.md](#)（模块 开发者文档；类别 docs；类型 documentation）：本 PR 第二个核心新增页：开发者接入指南，明确“provider = PROVIDER\_CREDENTIALS 注册项”契约，并给出四步接入流程与两层测试的分工说明。
- [examples/experimental/openenv/README.md](#)（模块 示例文档；类别 docs；类型 documentation）：重复信息最多的清理对象：删除逐 provider 的凭据参数表，保留 provider 特有行为（模板预构建、agentenv 别名、e2b>=2.12 约束），参数表凭据行合并为指向新文档的链接。
- [scripts/sandbox\\_smoke/README.md](#)（模块 冒烟脚本；类别 docs；类型 documentation）：删除“Exercised so far”运行记录表（harbor × e2b、harbor × daytona 的 PASS 记录）与重复凭据说明，实测组合记录迁移到用户侧网格，并补充注册测试的说明。
- [examples/experimental/harbor/README.md](#)（模块 示例文档；类别 docs；类型 documentation）：Validation 段落从“带日期与机型的运行日志”压缩为一句端到端结论，具体 provider 实测记录交给网格；同时保留并调整 --save-dir 磁盘空间警告的位置。
- [docs/docs.json](#)（模块 文档导航；类别 config；类型 configuration）：导航注册两个新页面：[user-guide/sandbox-providers](#) 挂到 Agentic Environments 分组、[developer/adding-a-sandbox-provider](#) 挂到 Developer Guide 顶层，保证站点可发现性。
- [docs/user-guide/environments.md](#)（模块 用户文档；类别 docs；类型 documentation）：回归 connector 索引定位：删除内嵌的 provider 使用表格，改为指向 [sandbox-providers](#) 页面的链接，明确 provider 是与 connector 不同的轴。
- [tests/e2e/agentic/test\\_harbor\\_rollout.py](#)（模块 端到端测试；类别 test；类型 test-coverage）：docstring 把“which combinations have been run”的引用从 [scripts/sandbox\\_smoke/README.md](#) 改为 [docs/user-guide/sandbox-providers.md](#) 的表格，保证实测记录只有一份。

- tests/e2e/agentik/test\_sandbox\_golden.py (模块 沙箱测试; 类别 test; 类型 test-coverage) : 与 test\_harbor\_rollout.py 相同: docstring 引用从 smoke README 改为新文档表格, 与开发者指南中“实测组合看网格”的表述保持一致。
- docs/user-guide/openenv.md (模块 用户文档; 类别 docs; 类型 documentation) : provider 列举从可读的四种名称收敛为指向 sandbox-providers 页面的链接, 并保留“共享 Docker env server”的补充说明。
- docs/user-guide/harbor.md (模块 用户文档; 类别 docs; 类型 documentation) : 链接引用微调 (+1/-1), 与新页面保持一致。

关键符号: 未识别

## 评论区精华

review 中无实质设计交锋: claude[bot] 自动审查返回“Code review found no issues”, 未发现高置信度问题; Shi-Dong 手动审查给出“Great job, LGTM!”并批准合并。唯一的人工评论是作者通过 issue 评论触发的 @claude review。由于是纯文档 PR, review comments 为空, 所有疑虑已收敛, 结论为可直接合并。

- PR 整体审查结论 (other): 全部通过, 无未解决疑虑。

## 风险与影响

- 风险: 文档性风险 (无代码风险) :
  - 手工维护的实测网格易过期: docs/user-guide/sandbox-providers.md 的勾选靠人工更新, 若新组合跑通后无人补勾, 用户会低估可用面; 反之若只跑了 golden smoke 就勾选, 会稀释“真实 rollout”的语义。
  - 相对链接敏感: examples/experimental/openenv/README.md、scripts/sandbox\_smoke/README.md 均使用 ../../../../docs/... 相对路径, 示例目录一旦移动即失效。
  - 与凭据契约耦合: 文档细节 (如 Modal token pair、E2B 双端点) 绑定 miles/rollout/agentik/credentials.py 的字段语义, 后续 provider 演进 (例如 PR#3215 的存储配额 override) 若不同步更新, 会出现“代码已支持、文档已过期”的漂移。
  - 无回归、性能、安全或兼容性影响: 纯文档变更, 测试文件仅改 docstring, CI 行为不变。
  - 影响: 用户影响: 跑 sandbox 型 recipe 的用户只需看 sandbox-providers.md 一个页面即可完成 provider 配置, 配方类 README 显著变薄; 要接入新 provider 的开发者获得明确四步清单。系统影响: 零运行时行为变化, CI 检测无行为变化, 站点导航净增 2 页。团队影响: 文档维护者从“多处复制”改为“单点更新”, 后续 provider 功能演进 (Modal、Daytona、AgentENV 等) 的文档成本降低; 但新增了 1 个需要人工维护的实测网格。
  - 风险标记: 纯文档变更, 手工维护的实测网格易过期, 相对链接易失效, 与凭据契约耦合

## 关联脉络

- PR #3195 test(agent): run the sandbox tests on any provider, not just e2b: 本 PR 栈在其上: 3195 让沙箱测试由凭据注册表驱动、任意 provider 可测, 本 PR 把“实测组合记录”从 smoke README 迁到用户文档, 正是承接 3195 的成果。
- PR #3214 docs: Harbor runs on Modal: 同一文档区域: 补充 Modal 实测结论, 与 sandbox-providers.md 的 Modal 配置与网格勾选直接相关。
- PR #3215 harbor daytona: reclaim orphaned sandboxes by default, and a storage override: 同批 provider 支持演进: 其存储配额配置语义与本 PR 新增的 provider 配置文档 (Daytona 磁盘配额提示) 相关, 后续需同步文档。
- PR #2876 ci(e2e): Harbor trials on real e2b sandboxes through the full rollout path (manual for now): test\_harbor\_rollout.py 测试线的起点, 本 PR 更新了该文件 docstring 的引用。
- PR #2837 docs: the in-process Harbor example: harbor README 文档的上一版本, 本 PR 继续精简其 Validation 段落并引入统一 provider 文档。