

如何约 200 元一年的基础设施

搭建小团队 AI 协作平台

DeepSeek Harness 多账户工作台的架构、实现与验证

● 一台轻量 VPS • 三个独立账户 • 一套共享能力



这份案例分五个部分

- | | | |
|----|--------|---------------------|
| 01 | 为什么要搭建 | 低成本试验场与三人研究团队 |
| 02 | 平台怎样工作 | 架构、协作边界、Cordis 与工具 |
| 03 | 我们踩过的坑 | 账户隔离、Office 取舍、插件适配 |
| 04 | 怎样证明可靠 | 五层验证与项目反思 |
| 05 | 接下来做什么 | 轻量协作、适用范围与联系方式 |

先看平台，再看取舍；最后讨论证据和下一步。

约 200 元的基础设施，足够搭起一块试验场

≈ ¥200

一年服务器预算

用低成本验证课程、科研和团队协作中的 AI 用法。先跑通，再决定是否扩大投入。



课程教学

尝试图形 Agent 与终端 Agent



科研实验

共同资料与个人分析分开



小团队协作

同一入口、独立会话、共享文件

约 200 元只指轻量服务器；模型调用、域名和维护人力另计。

一个三人研究团队，三个自己的 AI 工作间



admin

课题负责人

管理平台与共同资料



user1

研究员

整理文献与撰写 Word



user2

研究员

分析数据与制作 PPT

共同资料、团队聊天、统一工具

共享工作成果，不共享私人会话和凭据。

一扇门，三个工作间，一间公共资料室



公网只开放 Gateway ; 三个 DSH 后端只在服务器内部可达。

哪些东西共享，哪些东西必须分开

公共资料室

- 共同文献和数据
- 团队聊天
- 阶段成果
- 共享目录版本快照
- @ai 对共同资料的只读问答

个人工作间

- 登录密码和模型密钥
- 个人 AI 会话
- 未完成的草稿
- 个人任务看板
- 账户自己的终端进程

团队协作不是把所有内容放到同一个账号里。

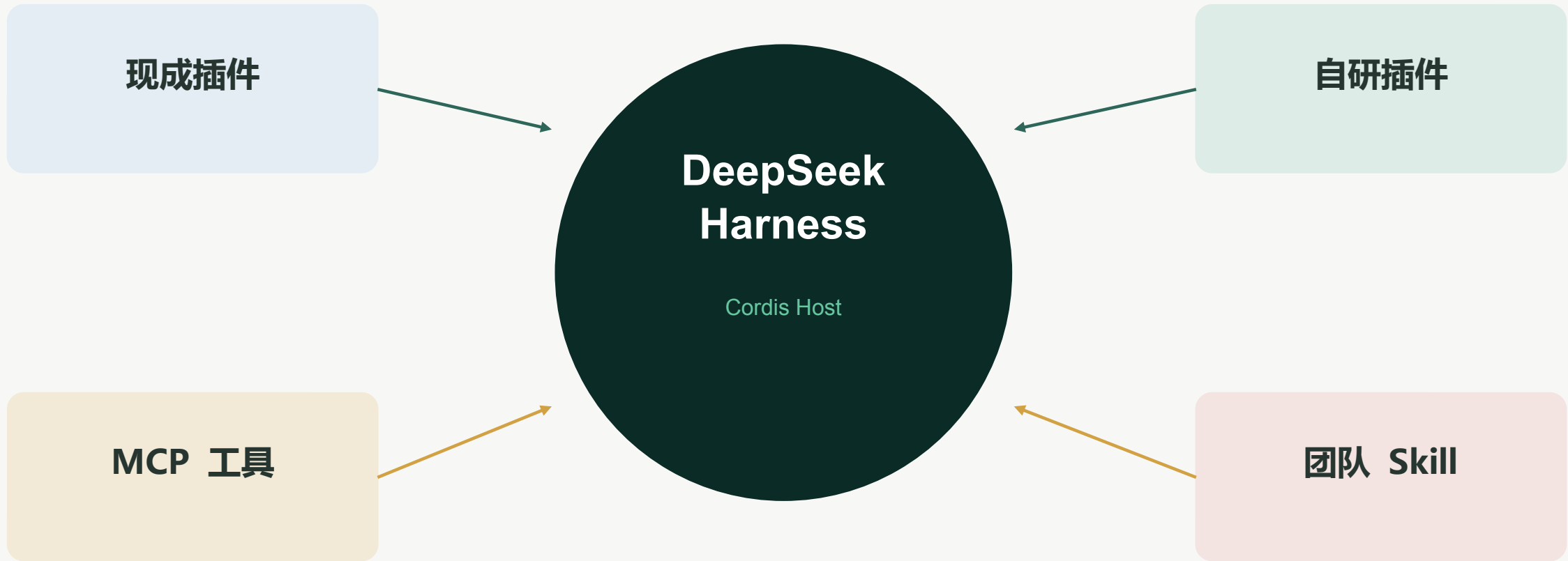
团队现在怎样完成一次共同任务



共同资料和讨论在团队层；思考过程、草稿和凭据留在个人层。

Cordis 是什么：Harness 的插件底座

Cordis 是 DeepSeek Harness 内部的插件框架，负责加载插件、连接服务并管理依赖。



功能按需组合，可以替换、禁用和升级；核心保持稳定。



Cordis 把聊天界面扩展成了工作环境

新会话

任务看板

1 任务与工具入口

技能中心

工作区

搜索

2 可复用的 Skill

生成Excel测试文件预览下载 5分钟

我的模型不支持直接看图，改用 describe_image 视觉分析工具逐页检查。

Tool call · describe_image · slides/slide-1.png

Tool call · describe_image · slides/slide-2.png

3 Agent 调用工具

Think · The vision model's analysis of slides 1 and 2:

第 1、2 页检查通过。继续检查第 3、4 页。

Tool call · describe_image · slides/slide-3.png

Tool call · describe_image · slides/slide-4.png

Think · Two issues found by the vision model:

发现两个问题需要核实：① 第 3 页图表区域空白；② 第 4 页卡片 3 右侧疑似有条状物。先验证 PPTX 里图表是否真实存在，并检查 HTML 预览的图表渲染机制。

Bash · Verify chart in pptx and inspect HTML chart rendering

Think · Findings:

PPTX 里图表是原生存在的 (chart1.xml)，文件本身没问题——是 officecli 的 HTML 预览不支持渲染 pptx 原生图表。我尝试用 SVG 模式渲染第 3 页，看它能否画出图表。

Bash · Test SVG mode page filter and chart rendering

Think · Interesting! SVG mode supports --page, and page 3 SVG mentions "column" (grep found 'column'). 4...

SVG 模式支持分页且第

Deep diving... 5分17秒

给智能体发消息

+ Workspace Write

DeepSeek-V4-Flash High

沙箱模式：已启用 · 页面无法访问界面数据与本地文件，登录态与第三方 Cookie 可能不可用 临时解锁 (不安全)

4 成果直接预览

QUARTERLY REVIEW · 2025 Q2

季度产品报告

市场与销售数据回顾 · 内部测试演示

TEST DECK

DeepSeek Harness 测试文件 · 2025 年 8 月

演示文稿，用于验证 PPT 生成与 HTML 预览功能。

关键数据一览

2025 Q2 · 截至 6 月 30 日

¥

1,284

季度营收 (万元)

+18.2% 环比增长

+

326

新增客户数

较上季度 +64 家

★

92.4

客户满意度 (分)

目标 90.0 已达成

同一个平台，能力来自四条扩展路径

● 现成插件

侧边栏、Skill 浏览、会话恢复、性能面板、个人任务看板

● 自研插件

团队聊天、成果下载、Office 预览、成果目录引导、网关适配

● MCP 工具

把 officecli 接给 Agent，用于 Word、PPT、Excel 的创建和检查

● 团队 Skill

把研究、引用核验、数据分析、文档制作和任务方法写成可复用流程

主要工作是选择、连接和补齐，而不是修改 Harness 核心。

插件不是越多越好：按工作需要分组

文档与成果

Office 预览

成果下载

成果目录引导

图片理解

工作环境

文件侧边栏

终端与 SSH

Skill 浏览

会话恢复

观察与管理

性能面板

Git 图

归档管理

插件诊断

团队协作

团队聊天

@ai 资料问答

共享目录

个人任务看板

真实包名和启用状态见演讲者备注。

同一工作台，两种 Agent 交互方式

1 图形界面：日常任务



2 终端：pi Agent TUI



终端适合进阶教学、复杂科研任务和排障；应按角色开放。

案例一：三个人能登录，不等于三个人能安全共用

最初看起来最省事

一个 DSH 进程
一个共享密码
三个人一起使用

会话、文件、任务归属和故障范围混在一起。



最后采用的办法

统一 Gateway
三个 OS 账户
三个独立 Agent

共同入口仍然简单，私人状态和资源边界真正分开。

案例二：放弃重型 Office 共编

Google Docs

部分成员访问不稳定

OnlyOffice / Collabora

3.3 GiB 主机余量不足

共享同一份 Office 文件

覆盖与责任难追踪



现在的文档循环

- 个人 Agent 起草
- officecli 生成与预览
- 共享目录交换成果
- 团队聊天提出修改
- Agent 生成新版本

少一个“炫”的功能，换来更低的资源占用和更清楚的责任。

坑三：插件装上了，公网入口却打不开



没有关闭安全检查；我们让内部代理符合插件原有的信任模型。

不能只看页面能不能打开

1

功能

登录、聊天、文件、
预览和调度

2

安全

跨账户读取、路径越
界、伪造请求

3

浏览器

公网 HTTPS、移动
端、断线重连

4

容量

三账户同时跑
Node、Office、传
输和 WebSocket

5

恢复

单实例重启、历史会
话、临时账户清理

三账户 30 分钟同窗测试：峰值合计约 895 MiB，未出现 OOM 或意外重启。

做完以后，我们改掉了四个想当然

01 大家协作，就该共用一切

私人会话和密码要分开；共同资料才共享。

02 插件装得越多，平台越强

插件确实省事，但要先看来源、权限和实际用途。

03 机器便宜，只能做简陋系统

真正需要的是取舍，不是把所有功能都塞进去。

04 AI 写完代码，页面能开就算完成

多人同时使用、越权尝试和重启恢复都要实测。

下一步不求更重，先把协作做得更顺



团队共享任务看板

现在三块个人看板互不相通。下一步由 Gateway 保存共同任务、负责人和执行账户。



Markdown 协作稿

共同编辑可比较、可恢复的 Markdown 源稿，定稿后转换成统一样式的 Word。



异地备份

当前恢复点仍在本机。增加远端存储，才能应对 VPS 整机丢失。



权限分层

普通成员使用图形界面；终端、插件安装和高级 TUI 按角色开放。

保留轻量架构，把真正缺少的团队层补上。

这套做法适合谁，也不适合谁

可以从这里开始

- 课程组、课题组和校内试点
- 3-5 人受信任小团队
- 以文献、数据和 Office 成果为主
- 接受单机维护窗口
- 愿意指定一位平台管理员

需要另一套架构

- 公开注册、计费和客户自助
- 互不信任的外部租户
- 必须多机高可用
- 严格跨地域灾备
- 完整实时 Office 共同编辑

一台小服务器， 先把团队的 AI 用法跑起来。

这个案例可用于课程实验、科研协作和校内小规模试点。

交流与合作

微信 hongyuatbj

