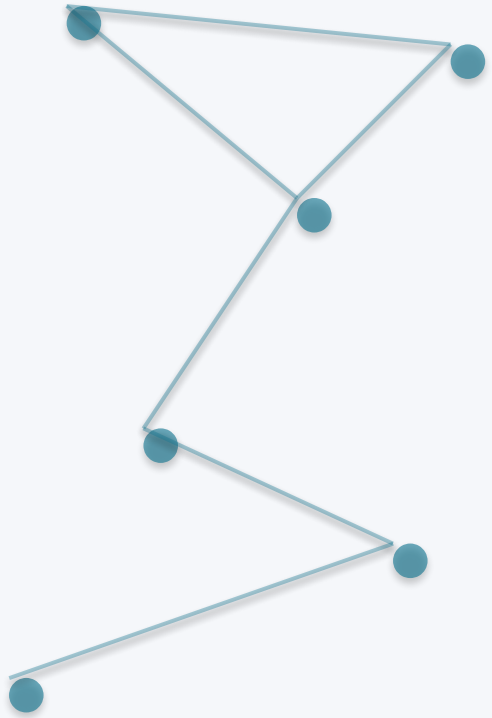
DeepSeek Harness

本地优先的 AI Agent 运行环境

Model + Harness = Agent



2026 年 8 月开源发布 | Apache 2.0 License

什么是 DeepSeek Harness？

DeepSeek Harness （dsh）是 DeepSeek 开源的本地优先 AI Agent 运行环境。
它不是一个模型，而是模型的“执行底座”——负责工具调度、上下文管理、
安全沙箱和插件编排，让 LLM 真正成为可操作的 Agent。

- 完全开源， Apache 2.0 协议
- 本地部署，数据不出境
- 模型可插拔，不绑定单一 LLM
- 全插件化架构，极致可扩展

Model + Harness = Agent

核心架构： Everything is a Plugin

基于 Cordis 框架，将 Agent 的每一层拆解为可替换插件

界面层	**Web UI** 本地浏览器交互	**CLI** 命令行界面	**API** 程序化接入
调度层	任务编排 多步工具调用	执行日志 追加式记录	分支 / 回溯 从任意点分叉
能力层	模型接入 可插拔 LLM	工具集 终端 / 文件 /Git	技能库 可复用流程
基础层	安全沙箱 隔离执行环境	存储 本地优先持久化	配置 密钥 / 插件 / 模型

插件生态系统

每个组件都是可替换的插件，通过 Cordis 统一注册和生命周期管理

模型插件

接入任意 LLM： DeepSeek 、 OpenAI 、本地模型等，统一接口屏蔽差异

工具插件

终端执行、文件系统、 Git 操作、网络请求等原子能力

技能插件

可复用的多步骤工作流，类似 Agent 的“记忆”

存储插件

本地优先的持久化层，支持上下文和会话管理

沙箱插件

安全隔离的代码执行环境，防止 Agent 越权

调度插件

任务编排与执行策略，控制工具调用顺序和并发

四种运行模式

01

标准模式

Standard

日常开发与问题修复，交互式对话，逐步工具调用

适用：代码编写、 Bug 修复、文件操作

02

代码模式

Code

将多步工具调用编写为脚本一次性执行，减少交互开销

适用：批量操作、自动化流程

03

极简模式

Minimal

最小化运行环境，去除 UI 和额外插件，纯 API 调用

适用：评测、 CI/CD 流水线、自动化测试

04

开发者模式

Developer

完整调试信息，插件热加载，开发者工具链集成

适用：插件开发、框架扩展、调试

执行日志系统

持续追加的结构化日志，让 Agent 的每一步都可追溯、可分支、可重放

1

继续执行

从上次中断处恢复，无需重新开始。日志完整记录每次工具调用的输入输出。

2

分支探索

从日志中的任意节点分叉，探索不同的解决路径，而不丢失原有进度。

3

历史回看

完整回顾 Agent 的思考过程和决策链，便于调试和优化。

```
$ dsh run --mode standard

[14:02:01] tool:read_file
  ↳ src/main.py (42 lines)
[14:02:03] tool:terminal
  ↳ pytest tests/ -v
[14:02:08] ✓ 3 passed, 1 failed
[14:02:10] tool:write_file
  ↳ src/main.py:fix bug #42

  └── branch: try-alt-approach
    [14:05:00] tool:terminal
    ↳ git stash && git checkout
```

快速上手

方式一：一键启动（推荐）

```
# 无需全局安装，npx 直接运行
npx @deepseek-ai/dsh web

# 或指定模式
npx @deepseek-ai/dsh --mode code
npx @deepseek-ai/dsh --mode minimal
```

方式二：从源码构建

```
git clone https://github.com/deepseek-ai/dsh
cd dsh && pnpm install
pnpm run build
pnpm dsh web
```

配置示例

```
# dsh.config.yaml
model:
  provider: deepseek
  name: deepseek-chat
  apiKey: ${DEEPSEEK_API_KEY}

plugins:
  - terminal
  - filesystem
  - git
  - web-search

sandbox:
  enabled: true
  allowedPaths:
    - ./workspace
```

竞品对比

DeepSeek Harness

开源 · 本地优先 · 全插件化

01 完全开源
Apache 2.0，可私有部署

02 模型可插拔
不绑定单一 LLM 厂商

03 极致可扩展
Cordis 插件架构，万物皆插件

04 本地优先
数据不出境，隐私可控

Claude Code

开箱即用 · 云端优先

01 开箱即用
无需配置，体验流畅

02 模型绑定
仅支持 Anthropic 模型

03 云端依赖
数据经过第三方服务器

04 扩展有限
插件生态相对封闭

Codex / Copilot

IDE 集成 · 生态依赖

01 IDE 深度集成
与编辑器无缝配合

02 生态丰富
大量第三方扩展

03 云端依赖
需要稳定网络连接

04 厂商锁定
绑定特定平台生态

总结

开源透明

Apache 2.0
完全可审计

本地优先

数据不出境
隐私可控

全插件化

Cordis 架构
万物皆可替换

模型无关

自由接入
任意 LLM

DeepSeek Harness 代表了 AI Agent 基础设施的开源方向：透明、可控、可扩展。

GitHub: github.com/deepseek-ai/dsh | Docs: dsh.deepseek.ai