OPEN-SOURCE AGENT INFRASTRUCTURE

DeepSeek Harness

一切皆插件的开源 AI Agent 基础设施

Cordis 微内核 | MIT 开源 | 开发者预览 v0.1

由 DeepSeek AI 构建 · npx @deepseek-ai/dsh web

含 AI 生成

目录

CONTENTS

01
认识 Harness
定义与核心定位

02
Agent = Model + Harness
模型与框架的分工

03
Cordis 插件架构
一切皆插件

04
四种运行模式
Standard / Code / Minimal / Creator

05
可观测与高性能
Trajectory 追溯与 KV Cache

06
安全、生态与上手
沙箱契约、场景与快速开始

什么是 DeepSeek Harness

由 DeepSeek AI 开源的生产级 AI Agent 执行框架（命令行 dsh）。它以「一切皆插件」架构为核心，由 Cordis 微内核驱动，统一管理智能体与真实环境的交互、工具契约、上下文流转与沙箱隔离。

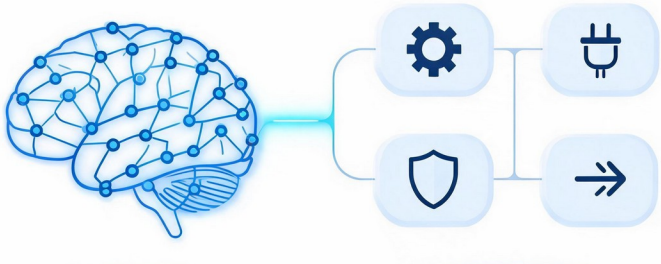
npm 一键启动
npx @deepseek-ai/dsh web，秒级拉起 Web UI

MIT 开源协议
完整源码开放，支持本地与企业云私有部署

开发者预览 v0.1
快速迭代中，核心插件与 API 持续演进



Agent = Model + Harness



模型负责思考，Harness 负责行动

Model · 模型 = 推理引擎

大模型提供认知与推理能力，是智能体的「灵魂」——决定下一步想什么、怎么决策。

Harness · 框架 = 控制中枢

让智能体理解环境、安全调用工具，并在真实环境中持续工作：

- 环境交互
- 工具契约
- 上下文流转
- 沙箱隔离
- 长期记忆
- 循环调度

Cordis 微内核：一切皆插件

Agent 能力插件层

模型 Models | 工具 Tools | 技能 Skills | 会话 Sessions | 沙箱 Sandboxes

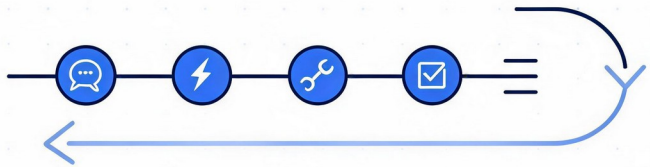
存储 Storage | 循环 Loops | 调度 Scheduling | 界面 UI

Cordis 服务与事件总线 · Services & Events

Cordis 微内核 —— 插件加载 · 卸载 · 生命周期与依赖路由

在 YAML / JSON 配置中选择、替换、扩展任意能力 —— 无需改动 Harness 源码

每次运行，皆可追溯



Append-only 会话事件流

- 系统提示与每一次上下文注入
- 模型推理过程（Think）
- 工具调用参数与执行结果
- 子智能体（Subagent）调度

同一事件流上的四种操作

恢复	分叉	搜索	重放
Resume	Fork	Search	Replay

黑盒 Agent 的完整审计与调试能力

四种预设模式，覆盖不同工程工作流

Standard

全功能编码 Agent

文件编辑与 diff 替换、Shell 、文件与网页搜索、技能、规划、目标、子智能体与工作流，开箱即用。

Code / PTC

程序化工具编排

通过 Code Mode SDK 暴露工具，模型用一段 TypeScript 表达多步循环与条件逻辑， Token 开销更低。

Minimal

零噪声基准评测

仅保留持久化 bash 与 str_replace_editor 两个工具，剔除提示噪声，为 SWE-bench 等提供干净环境。

Creator

内存插件实验室

检查当前运行时，在内存中热试验 Cordis 插件，并将其组合保存为自定义 Agent 预设。

原生 KV Cache 优化：高吞吐、低成本

99.93%

前缀缓存命中率

深度对齐 DeepSeek 原生 Prefix Cache 架构

80%+

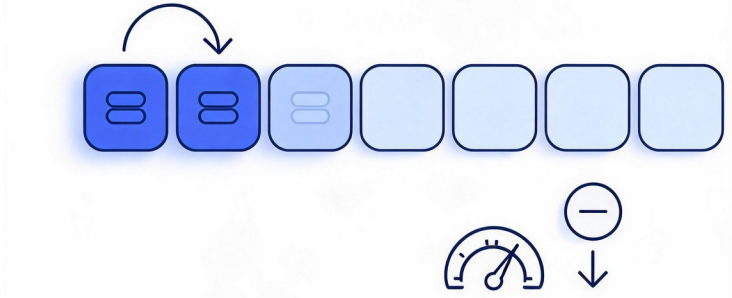
Token 成本下降

更低

多轮请求延迟

命中机制

- 严格的提示词前缀顺序
- 固定系统工具契约定义
- 增量对话历史分块缓存



前缀复用 · 消除冗余上下文重算

工具契约、沙箱隔离与基准评测

工具契约 + Docker 沙箱

无歧义 TypeScript 工具契约；高精度多块 diff 无损代码替换；容器隔离执行，严格约束路径访问边界与权限。

DSBench 自动化评测套件

开箱即用 DSBench / LM-Eval 运行器，实时写入 Trajectory 事件流，支撑自动化 CI/CD 回归测试与 RL 反馈对齐。



安全执行 · 精确编辑 · 可回归

谁在用 Harness 做什么



01 全栈编码自动化

Standard 模式：文件编辑、 Shell 、语义搜索、技能与子智能体协同，开箱即用

02 程序化工具编排

Code / PTC 模式：用 TypeScript 编排多轮工具调用，表达复杂循环与分支

03 模型基准评测

Minimal 模式：双工具零噪声环境，跑 SWE-bench 、 DSBench 等评测

04 插件生态与审计

Creator 模式开发 dsh-plugin ； Trajectory 支持全链路审计、分叉与重放

两条命令，即刻开始

npm 一键启动

```
$ npx @deepseek-ai/dsh web
# Web UI → http://127.0.0.1:3080
```

从源码运行

```
$ git clone deepseek-ai/deepseek-harness
$ pnpm install && pnpm run build
$ pnpm dsh web
```

GitHub 仓库

deepseek-ai/deepseek-harness

开发者文档

deepseek-harness.github.io

社区插件

GitHub Topic: dsh-plugin

运行前请阅读仓库安全说明 SAFETY；开发者预览阶段可能出现破坏性变更。

与全球开发者一起

探索智能的边界

开源 · 可组合 · 可复用的 Agent 基础设施

github.com/deepseek-ai/deepseek-harness · MIT License

Thank You

AI生成