DeepSeek Harness

开源智能体框架介绍

产品能力、插件架构与上手方法



2026.10

DeepSeek Harness 是什么

一个把模型、工具与工作区组织在一起的开源智能体框架

模型负责判断下一步，Harness 组织任务执行。

模型

理解目标，生成内容
选择下一步要调用的工具

Harness

准备上下文，调度工具
记录过程，管理任务状态

工作成果

修改后的代码与文件
分析结果、文档和任务报告

可通过桌面应用使用，也可启动本地 Web 界面。

一次任务如何执行

示例任务：定位一个报错，修复代码，并运行相关测试

01

理解任务

读取工作区资料
明确目标与限制

02

调用工具

请求读取文件、
编辑代码或执行命令

03

读取反馈

将工具结果加入上下文
决定是否继续下一步

04

交付结果

整理修改与验证结果
说明尚未解决的问题

工具结果会进入下一次模型请求，任务可以连续执行多个步骤。

核心设计：一切皆插件

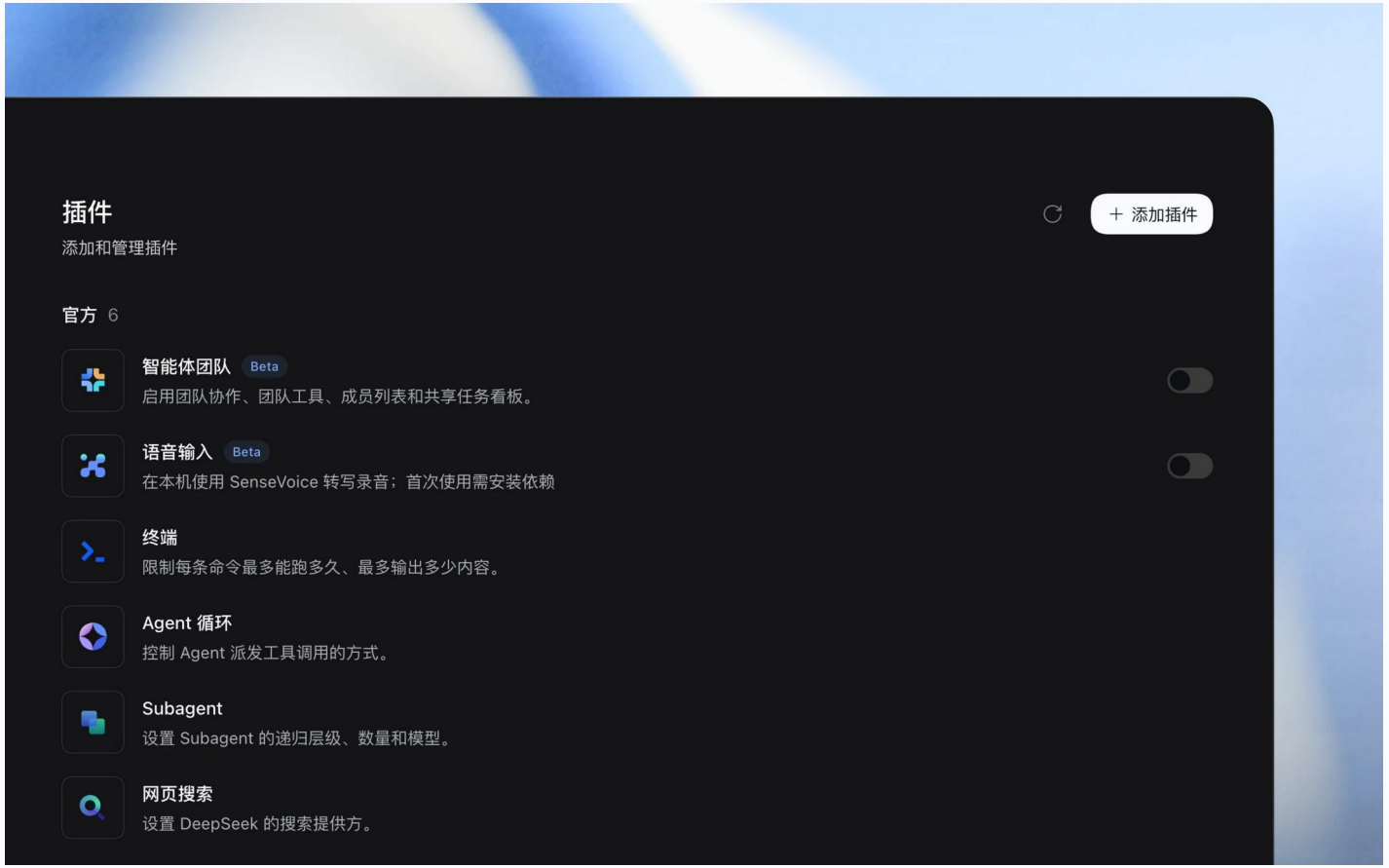
按任务需要组合能力，也可以替换已有实现

可组合

把工具与工作流程
按自己的需求装配

可替换

模型适配器、会话日志
和 Agent 循环都属于插件



底层架构的四个主要部分

Cordis 为插件提供共享上下文、服务注册与生命周期管理

组成	主要职责	可以扩展的内容
模型接入	把请求发送给选定模型	模型提供方与调用适配器
Agent 循环	组织请求与后续工具执行	任务执行策略与事件处理
工具与执行环境	提供文件、命令等操作能力	工具、文件系统和执行后端
会话日志	保存任务的持久事件	会话存储、恢复与历史投影

扩展能力通常通过插件接入已有接口。

典型应用场景

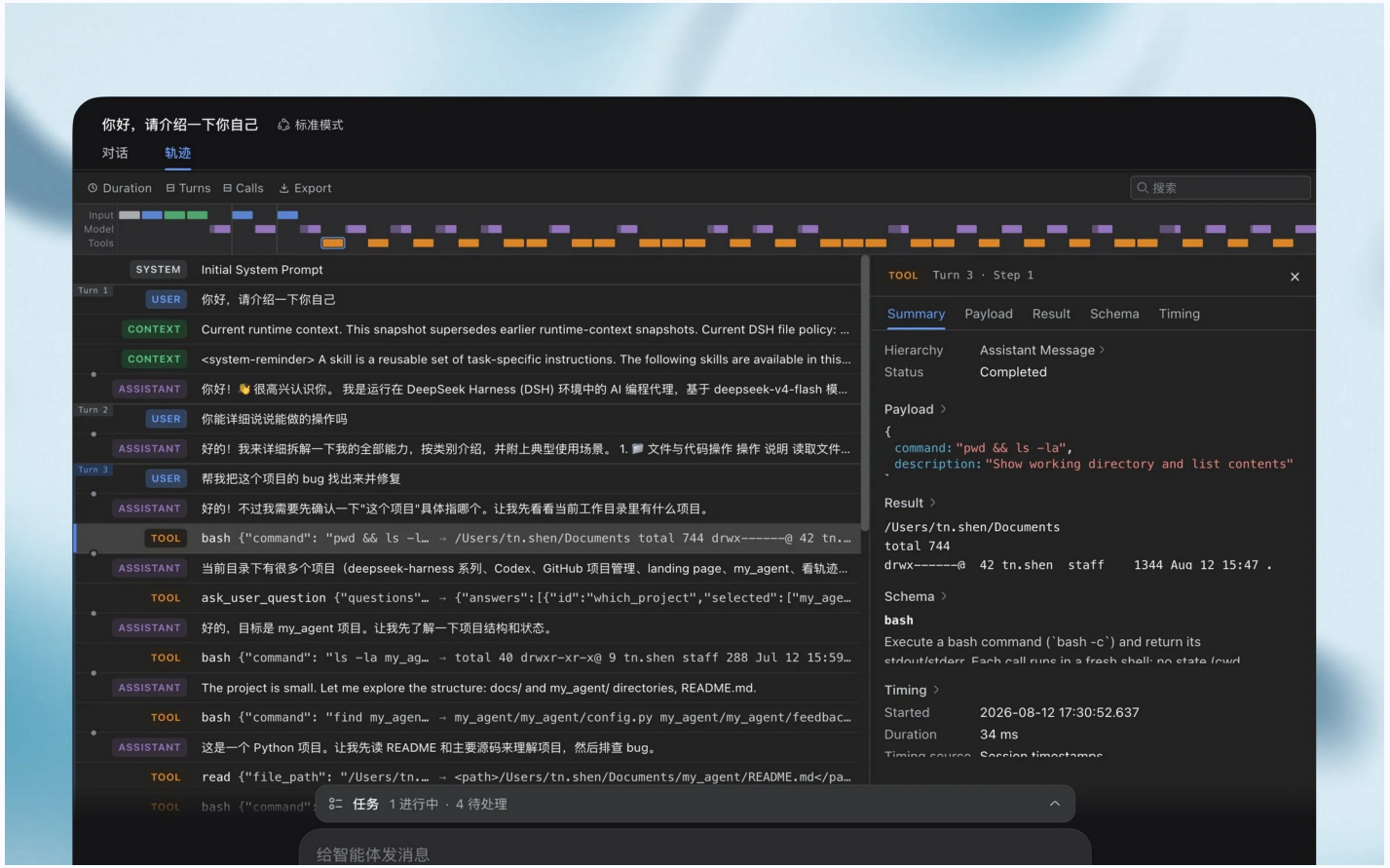
以下为能力对应的示例任务，实际效果需要在自己的工作中验证

	工作类型	可以交给它的任务	预期交付物
01	**代码开发**	修复问题、开发功能、运行测试	代码改动与测试结果
02	**资料研究**	检索资料、交叉核对、整理结论	附来源的研究摘要
03	**日常办公**	整理文档、分析表格、制作汇报	可继续修改的工作文件
04	**重复工作**	运行脚本、批量处理、计划执行	批处理结果或定期报告

计划执行需要启用自动化任务插件，并按具体环境配置。

执行轨迹让过程可追溯

按时间线查看模型请求、工具调用和返回结果



定位问题

查看哪一步停滞，
工具返回了什么

理解过程

结合轮次、输入与结果，
检查执行是否符合预期

扩展能力的两条路径

现有插件可直接安装，新的需求也可以做成插件

通过对话创建

创造模式

描述想要的功能，
让 Agent 协助生成并安装插件。

官网示例：番茄时钟悬浮插件

通过代码开发

开发者扩展

通过上下文注册工具或服务，
声明依赖并管理资源生命周期。

适用于团队工具和业务系统接入

模型接入可以按环境选择

在“设置 / 模型”中配置提供方，随后选择会话使用的模型

接入方式	适用情况	配置要点
DeepSeek	使用 DeepSeek API	填写并保存 API 密钥
内置第三方提供商	接入已支持的其他模型服务	选择提供商并填写凭据
自定义模型 API	公司网关、自建服务或中转端点	填写地址、协议与模型 ID

本地运行 Harness，与模型在哪里推理，是两个独立的配置问题。

接口能否工作，取决于模型能力和端点协议兼容性。

第一次使用的基本步骤

可从官网下载桌面端，也可安装 Node.js 后启动本地 Web UI

```
npx @deepseek-ai/dsh web
```

默认访问地址 http://127.0.0.1:3080

01 **配置模型** 在设置中保存 API 密钥，选择可用模型

02 **选择工作区** 添加并选中一个用于试用的项目目录

03 **发起任务** 写清目标、允许修改的范围和验收标准

首个任务示例：总结这个仓库的结构，并列出主要模块。

当前阶段与试点建议

项目仍在开发者预览阶段，接口与行为会继续迭代

当前需要了解

版本兼容性

官方明确提示可能发生破坏兼容性的变更

执行权限

可执行代码、读取文件并加载第三方插件
官方尚未将其视为生产就绪软件

建议的试点方式

从可回滚的任务开始

使用独立工作目录，授予所需权限
先人工复核，再扩大自动化范围

观察四项结果

完成质量、人工返工、耗时与调用成本

可组合的智能体工作环境

DeepSeek Harness 的价值，在于把模型能力组织成可持续执行的任务

用现成能力完成工作

在工作区中读取、修改、验证并交付结果

用插件适配自己的流程

按需求扩展工具、接入模型或调整执行方式

继续了解

产品官网

GitHub 仓库

开发者文档

安全与使用说明

资料截至 2026 年 10 月 3 日。详细来源见各页演讲者备注。