ASTRON AGENT · 开源企业级 Agentic 平台

v1.0.9 版本更新解读

主题：独立 Agent 的一次重大升级 —— 运行时、能力、协作、文档全面进化

01 独立 Agent 增强

02 协作与工作台

03 文档与示例

04 安全与稳定

2026-06-18 · github.com/iflytek/astron-agent/releases/tag/v1.0.9

v1.0.9 更新总览

本次发布是对独立 Agent 的一次系统性升级，覆盖四个方向。

① 独立 Agent 增强

运行时迁移到 Spring AI；新增自定义 MCP 接入；Skill 模块（最多 30 个，read_skill / run_skill）。

② 协作与工作台

团队发布审批流（OWNER/ADMIN 审核）；工作台改版；调试会话历史 + 联网搜索改进。

③ 文档与示例

VitePress 文档国际化标准化；社区工作流示例画廊 + 提交模板；FAQ 社区问答补充。

④ 安全与稳定

代码扫描安全加固；收紧 Agent 工具调用边界；修复顺序依赖的 toolkit 测试。

变更量：248 个文件 · +18,358 / −6,136 行

模块 ① · 核心

独立 Agent 增强

运行时换成 Spring AI 标准实现，新增自定义 MCP 接入，并让 Skill 成为一等能力。

1 运行时重构：手写运行时 → Spring AI

重构前 · 手写运行时

- PromptChatService ≈ 1690 行
- SparkChatService ≈ 764 行
- 手动编排工具调用
- 与模型强耦合，扩展困难

重构后 · Spring AI 运行时

- OpenAiChatModel + ToolCallback 标准实现
- 动态创建 OpenAI 兼容模型客户端
- 工具拆为标准回调：web_search / current_time / MCP
- 复刻旧版流式 SSE 协议，前端无感知

1 自定义 MCP 接入与用户价值

−2400+ 行手写运行时删除

+8 个 springai 组件

≤30 个可挂载技能

自定义 MCP 运行时工具

能力页填写 MCP Server URL，接入外部 MCP 工具；模型按工具描述自主选择调用。McpRuntimeToolService + McpToolCallbackFactory。

用户能看到什么

- 能力配置里填自定义 MCP 地址，接第三方工具
- 流式输出更稳：取消 / 断连时及时停止
- 前端几乎无感知 —— SSE 协议被复刻

2 Skill 能力：持久化 → 读 → 执行

1 持久化 & 界面

能力页新增技能区块；选中技能以 JSON 存入 chat_bot_base.skills（最多 30 个）。

迁移 V1.38 · SkillSelectModal

2 运行时读技能

为每个技能注册 read_skill_{id}，Agent 可读技能文档；调试阶段实时注入。

SkillEnrichmentService

3 沙箱执行

新增 /skill/sandbox-exec，复用 E2B 沙箱执行命令；注册 run_skill_{id}。

skill_sandbox_api · AGENT_URL

2 两个新工具：read_skill 与 run_skill

read_skill_{id}

读取技能文档

- 对话中读取技能说明，理解它能做什么
- 解析下载地址、资源、沙箱配置
- 调试请求中实时注入 —— 不必先保存

run_skill_{id}

在 E2B 沙箱执行命令

- console-hub 通过 /skill/sandbox-exec 调用
- 复用经审计的 E2B 沙箱执行
- 返回 exit_code / stdout / stderr
- 沙箱未配置时优雅降级

模块 ② · 协作

协作与工作台

工作台改版、调试会话历史持久化，并新增面向共享空间的团队发布审批流。

1 工作台改版 + 调试会话历史

工作台重写

- CapabilityDevelopment 重写 ≈ 1533 行
- config-base 配置面板大幅重构
- 能力分区更清晰、交互更紧凑
- 联网搜索工具编排改进

调试会话历史持久化

- 新增 AgentDebugSession / AgentDebugMessage（迁移 V1.36）
- AgentDebugController + 服务层持久化调试对话
- 刷新 / 切走再回来，调试历史仍在
- 调 prompt → 看效果 → 再调，不丢上下文

2 团队发布审批流（共享空间 · 实测）

1. 成员发起发布 → 2. OWNER / ADMIN 审核 → 3. 通过后上架

共享空间「发布审核」控制台：列表含 申请人 / 审核人 / 状态 / 操作，发布需审核通过才上架。

模块 ③ · 生态与质量

文档、示例与安全稳定

文档国际化、社区示例画廊，以及一轮安全加固与稳定性修复。

1 文档与示例 · 安全与稳定

文档与示例

- VitePress 文档标准化 i18n，新增 editLink 与贡献指南
- 社区工作流示例画廊 + 提交模板（issue template）
- FAQ 补充社区问答，更新模型示例

安全与稳定

- 代码扫描安全检查加固（code scanning）
- 收紧 Agent 工具调用边界
- 修复顺序依赖的 toolkit 测试，重置共享配置状态

升级注意事项

必须显式选择模型

移除内置星火默认，升级后需为 Agent 显式配置模型

数据库迁移 V1.38

Flyway 自动新增 chat_bot_base.skills 列

配置 E2B 脚本沙箱

技能执行（run_skill）依赖 E2B 沙箱，需配置密钥

配置 AGENT_URL

打通 console-hub 到 core-agent 的沙箱通信

真实环境实测

本地部署 · 浏览器实拍

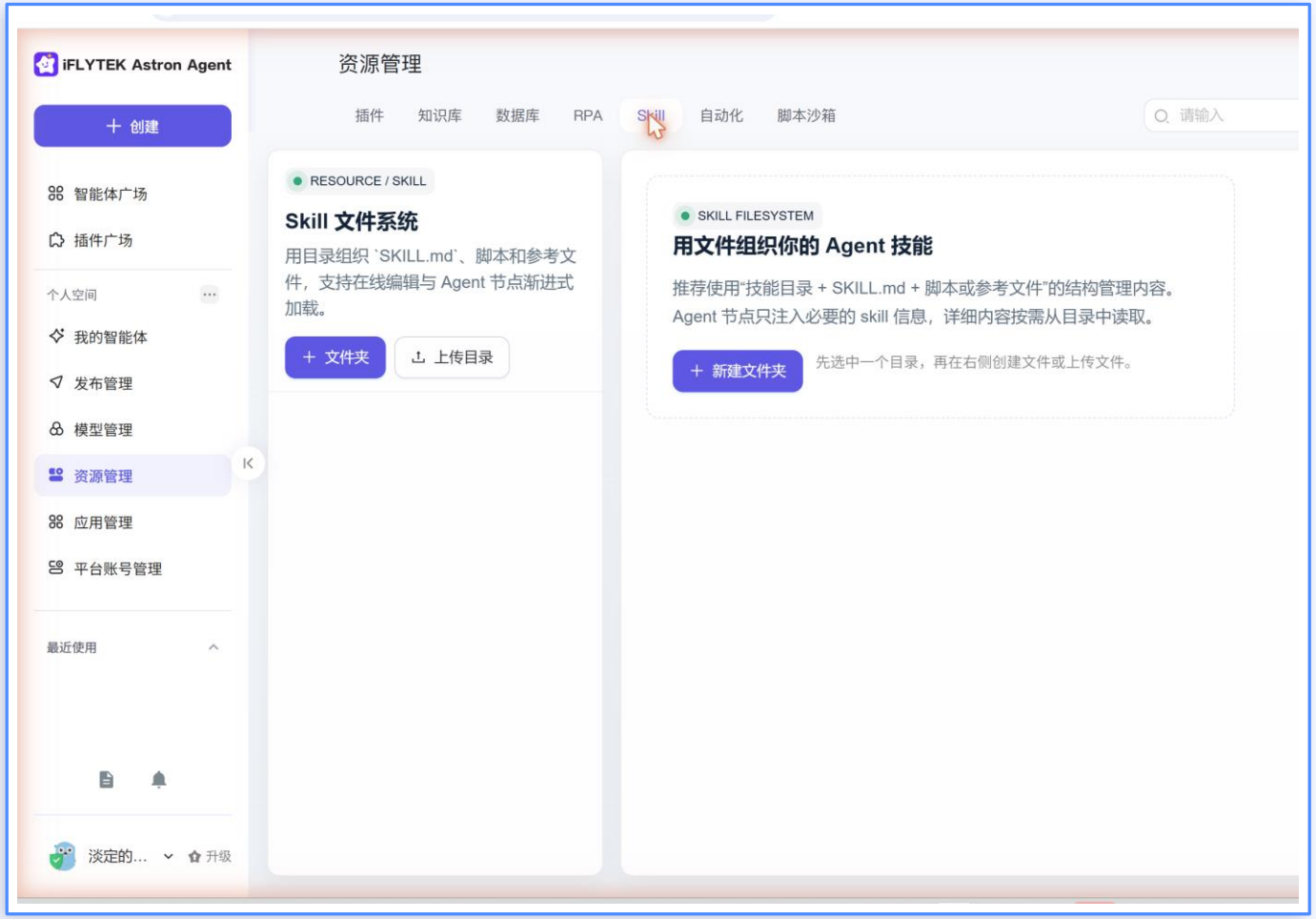
本地 docker-compose 部署 v1.0.9 并配置模型后实拍。运行时、Skill、工作台、发布审核均为真实截图。

1 实测 · 运行时（自定义 MCP + 工具调用）

能力页「MCP Server」可填自定义 URL

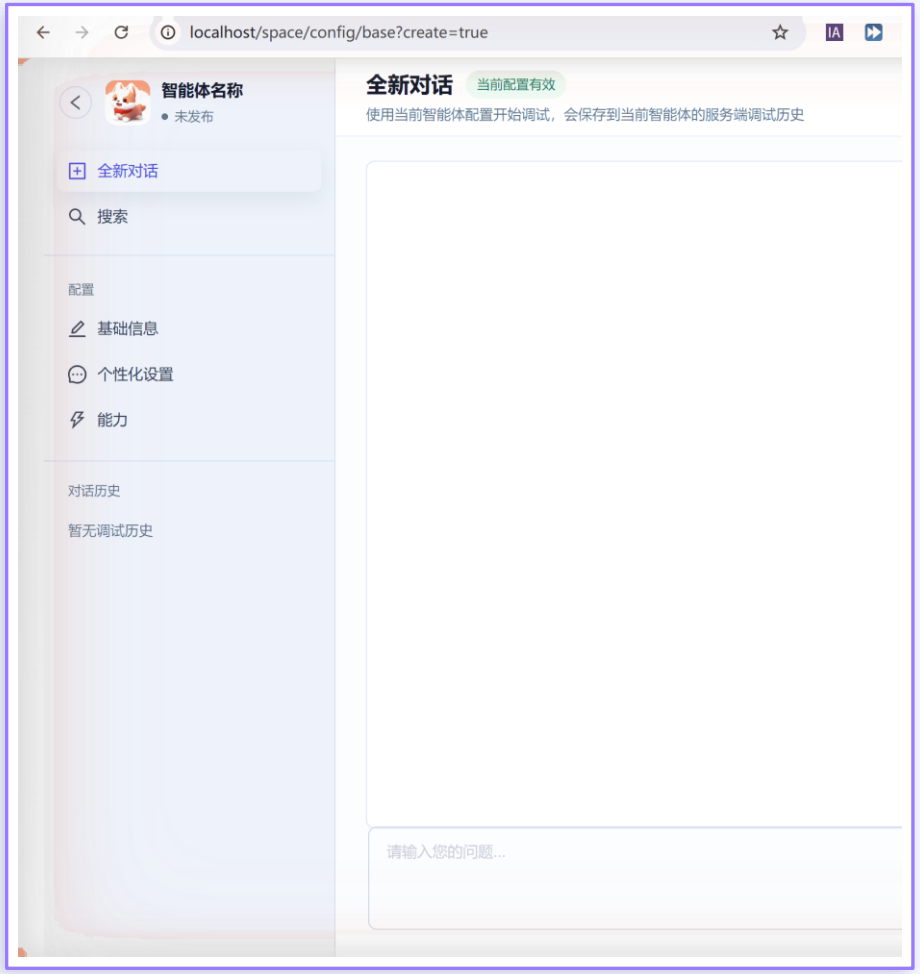
Agent 实际调用 current_time 工具并给出北京时间

2 实测 · Skill 资源（文件系统 / SKILL.md）



资源管理 → Skill：用目录组织 SKILL.md、脚本与参考文件；运行时 read_skill 读取、run_skill 在 E2B 沙箱执行（V1.38）

3 实测 · 改版工作台（配置分区 + 调试会话历史）



截图要点

- 左侧「配置」分区重排：基础信息 / 个性化设置 / 能力
- 独立「对话历史」面板 —— 调试会话服务端持久化（V1.36）
- 顶部「会保存到服务端调试历史」即该能力入口
- 中间为调试对话区，右上「创建 / 发布」

总结

v1.0.9 · 独立 Agent 的一次重大升级

①	独立 Agent 增强	Spring AI 运行时、自定义 MCP、Skill 能力（read/run）。
②	协作与工作台	工作台改版、调试会话历史、团队发布审批流。
③	文档与示例	VitePress i18n、社区工作流画廊、FAQ。
④	安全与稳定	代码扫描加固、工具调用边界、测试稳定。

升级请注意：显式选择模型 · V1.38 迁移 · E2B 沙箱 · AGENT_URL | github.com/iflytek/astron-agent