

BoardWare AI-Native & Sandbox Solutions

March 19th, 2026

博維聚力·智創未來

BoardWare Intelligence Innovates the Future

BoardWare TerraMind & Sandbox

大模型落地“最后一公里”的挑战

集成

- 无法直接操作企业内部 ERP、CRM、数据库等专业工具。

记忆

- 通用 LLM 无法长期记忆用户偏好及特定业务背景知识。

协同

- Agent 处于独立孤岛，缺乏跨岗协同及数据交换机制。

OCDP 全场景赋能矩阵 (三位一体)

应用层 (APPLICATION)

Agent Sandbox (业务智能)

服务层 (SERVICE)

Unified API Gateway (模型枢纽)

算力层 (INFRASTRUCTURE)

Cluster Management (算力基座)

MODULES CAN BE DEPLOYED INDEPENDENTLY OR AS A FULL STACK

個人智能體進化沙盒



私有化隔離

企業級安全沙盒，確保 Agent 處理的敏感數據物理隔離，不流出內網，保護商業秘密。



長期記憶能力

內置向量數據庫支持，Agent 可持續累積業務經驗與用戶偏好，形成長期的「專業化大腦」。



MCP & Skills

支持模型上下文協議（MCP），通過 Skills 技能池自由連接 ERP/CRM 或執行自動化腳本。

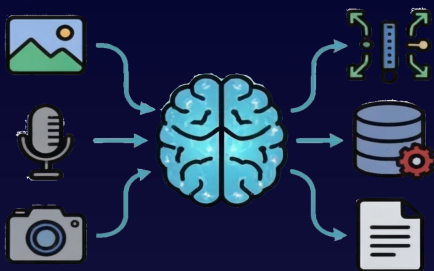


Agent Network

通過私有數據交換協議，開啟群體智能協同時代。

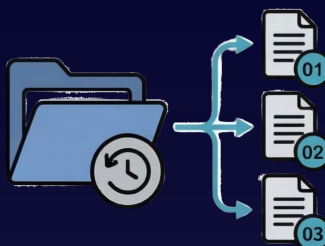


1. 多模態記憶



- **語義索引增強**：支持文字、圖片元數據及語音轉譯文本關聯索引
- **上下文演進機制**：自動壓縮短期對話轉入長期向量數據庫
- **分層記憶邏輯**：區分“事實性記憶”和“過程性記憶”

2. 可回滾追溯的文件系統



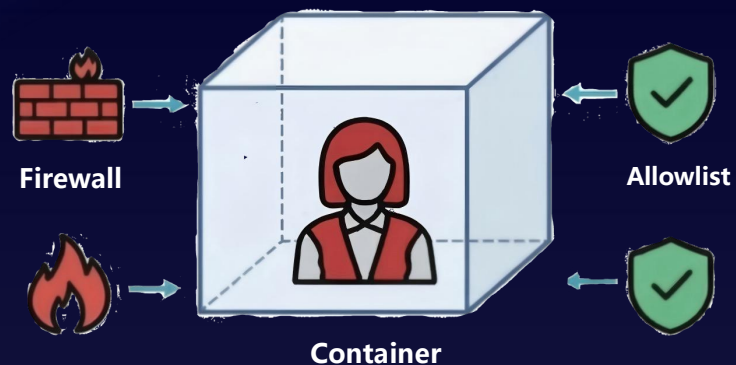
- **高性能文件系統**：提供企業級的私有化對象存儲
- **數據版本追蹤**：對Agent修改的文件生成版本記錄
- **合規與鎖定機制**：支持WORM模式配置

3. 私有化通訊Channels



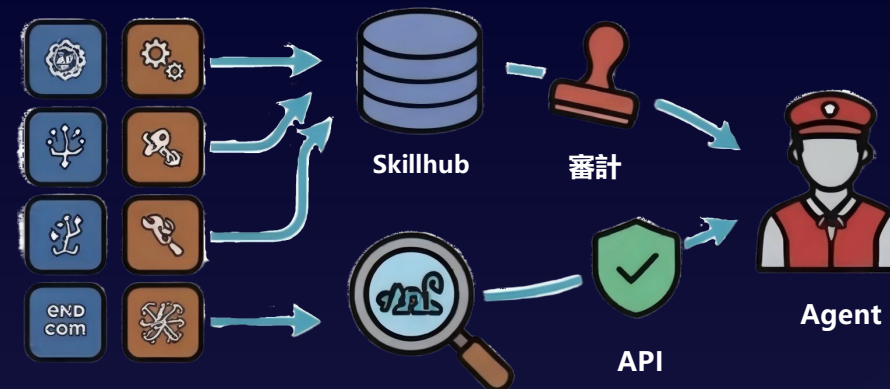
- **安全通訊基礎**：為Agent與用戶、Agent與Agent之間的通訊數據流轉建立安全鏈路
- **分佈式協同支持**：基於去中心化協議設計，支持私有化部署
- **多段集成潛力**：將Agent安全接入郵箱、飛書等平臺

4. 安全不越權的優化「內核」



- 輕量化沙箱容器：每個Agent運行在受控的Container隔離環境中
- 最小權限管理：默認禁用所有敏感系統調用，執行默認最小權限原則
- 資源隔離：確保每個Agent異常邏輯不會影響主機

5. 受信任可審計的Skillhub



- 動態服務發現與健康檢查：實時感知Agent和Skill的狀態
- 配置中心化管理：所有Prompt、Tool定義、API Key統一管理
- 技能審計：所有上綫技能必須經過審計及安全評估

1. 系統運營監控



- **智能日志異常診斷**：結合歷史故障模式，自動識別潛在風險並給出預警建議
- **安全沙箱故障修復模擬**：安全執行修復腳本或配置更改測試
- **自動化巡檢與健康審計**：利用動態服務發現機制生成具備版本追溯能力的巡檢報告

2. 個人辦公自動化助手



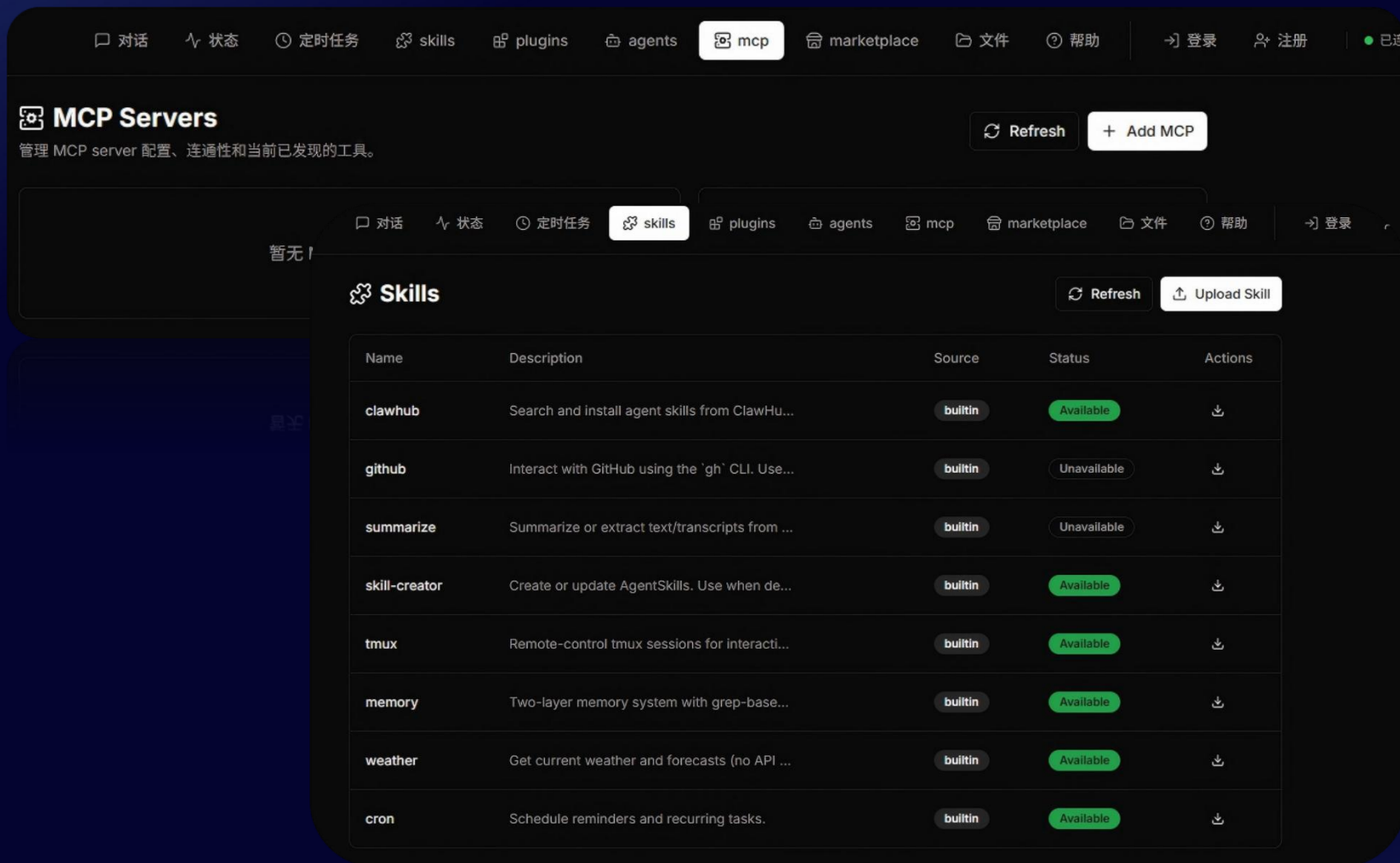
- **跨平台會議跟進與知識整合**：通過接入辦公軟件自動抓取對話細節協助進行信息整合
- **動態知識庫維護與回溯**：用戶利用可回滾文件系統管理個人工作文檔
- **定製化資訊深度洞察**：Agent 定時抓取行業資訊，結合用戶偏好提供精準行業信息

3. 科研助理



- **實驗環境自動化部署與隔離測試**：在受控及隔離的沙箱內自動完成實驗環境部署
- **科研數據流轉與版本控制**：高性能文件系統做數據存儲，支持隨時回滾到特定節點
- **文獻結構化檢索與交叉分析**：協助科研人員在海量資料中快速建立知識關聯與邏輯鏈條

Skills & MCP 管理界面



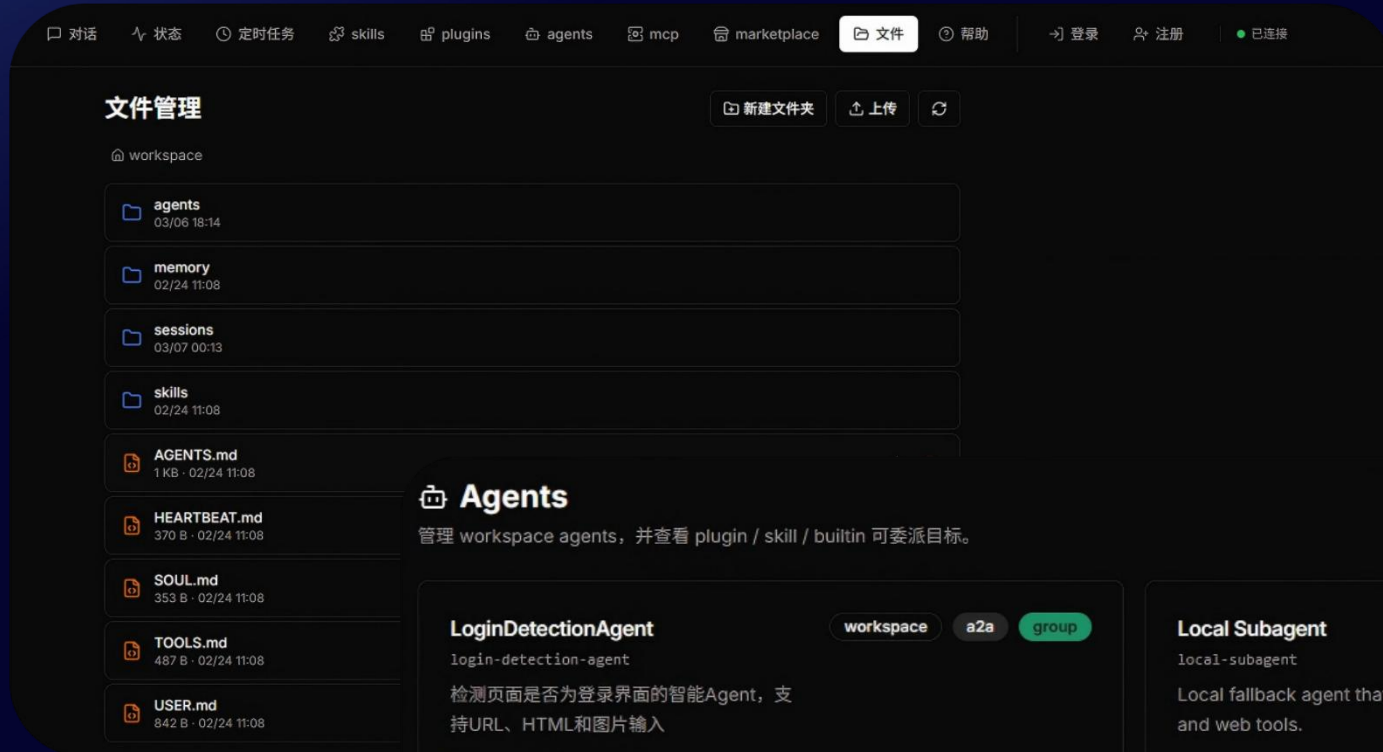
The screenshot shows the MCP Servers management interface. At the top, there is a navigation bar with tabs for '对话', '状态', '定时任务', 'skills', 'plugins', 'agents', 'mcp', 'marketplace', '文件', '帮助', '登录', '注册', and '已连'. Below the navigation bar, the 'MCP Servers' section is visible, with a 'Refresh' button and an 'Add MCP' button. The main content area shows a list of skills, with a 'Skills' tab selected. The skills list is as follows:

Name	Description	Source	Status	Actions
clawhub	Search and install agent skills from ClawHu...	builtin	Available	↓
github	Interact with GitHub using the 'gh' CLI. Use...	builtin	Unavailable	↓
summarize	Summarize or extract text/transcripts from ...	builtin	Unavailable	↓
skill-creator	Create or update AgentSkills. Use when de...	builtin	Available	↓
tmux	Remote-control tmux sessions for interacti...	builtin	Available	↓
memory	Two-layer memory system with grep-base...	builtin	Available	↓
weather	Get current weather and forecasts (no API ...	builtin	Available	↓
cron	Schedule reminders and recurring tasks.	builtin	Available	↓

功能展示及描述

- 用於設置自己的Skills,Mcp
- 後續可在市場添加新功能

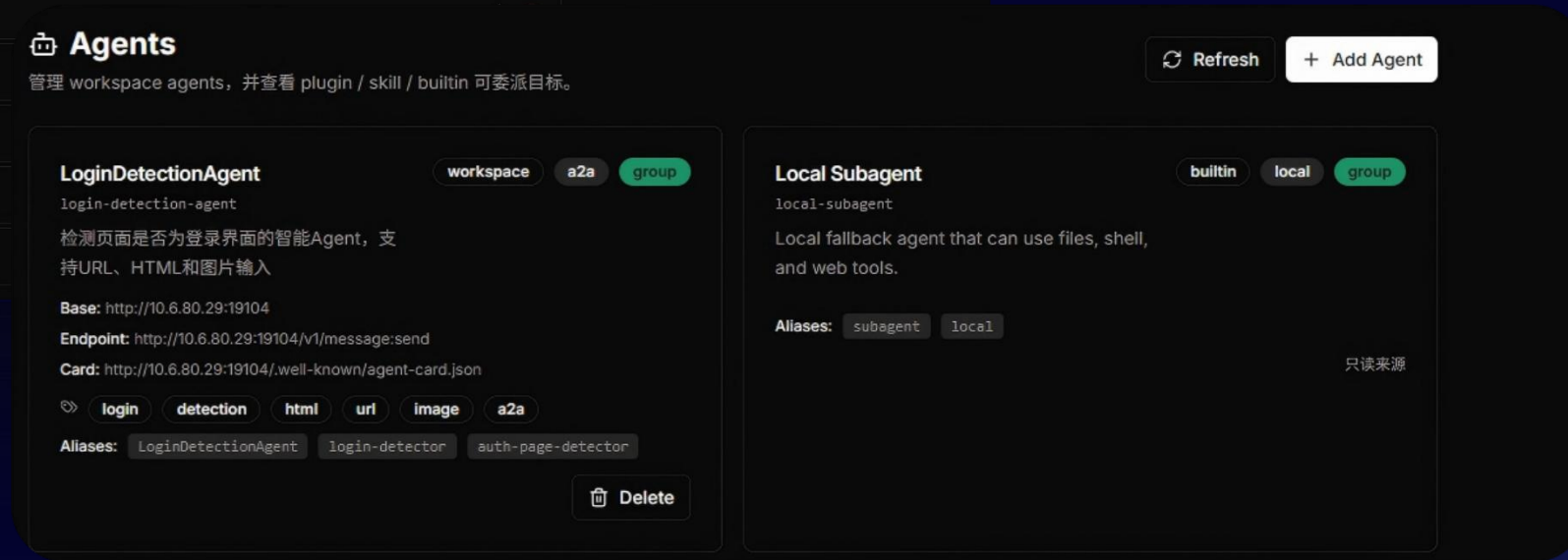
Agent 管理 - 文件系統



The screenshot shows the '文件管理' (File Management) section of the dashboard. It features a top navigation bar with various icons and a '文件' (Files) tab. Below the navigation, there are buttons for '新建文件夹' (New Folder), '上传' (Upload), and a refresh icon. The main area displays a list of files and folders within a 'workspace' environment. The files listed include 'agents', 'memory', 'sessions', 'skills', 'AGENTS.md', 'HEARTBEAT.md', 'SOUL.md', 'TOOLS.md', and 'USER.md', each with its size and creation date.

保證Sandbox私有化

- 附帶界面的獨立文件管理系統
- 設置Agent Group



The screenshot shows the 'Agents' management section. It has a 'Refresh' button and an 'Add Agent' button. Below these, there are two agent cards. The first card is for 'LoginDetectionAgent', which is currently in the 'group' state. It includes a description: '检测页面是否为登录界面的智能Agent, 支持URL、HTML和图片输入'. It also lists its 'Base', 'Endpoint', and 'Card' URLs, and its 'Aliases'. The second card is for 'Local Subagent', which is currently in the 'group' state. It includes a description: 'Local fallback agent that can use files, shell, and web tools.' and its 'Aliases'. A 'Delete' button is visible at the bottom of the first card.

三位一體驅動方案

全場景滿足客戶需求



OCDP 架構無縫整合運算能力、服務和應用程序，以智慧能力賦能各種業務場景。





Thank you !