M3 · 职业版 Agent · 第 5 讲

第 5 讲：企业级 Agent OS

五层结构，共享能力

阅读约 25 分钟

练习约 30 分钟

产出：架构与上线路径

本节目录

一个真实故障

本讲目标

一、五层结构

二、五个共享能力

三、多租户隔离

四、上线路径

五、30 分钟练习

六、验收清单

七、延伸阅读

一个真实故障

三个部门各搭了一个 Agent，各自接了 CRM。月底发现：客户被重复回访、报价口径不一致、同一个 API key 被用爆。

单个 Agent 是工具，多个 Agent 是系统。系统需要一层“操作系统”。

本讲目标

- 用五层结构描述企业级 Agent OS；
- 设计共享能力：网关、注册表、权限、审计、配额；
- 做多租户隔离；
- 规划从单团队到全公司的上线路径。

一、五层结构

层	内容	解决的问题
接入层	入口、身份、路由	谁在调用
编排层	任务拆分、队列、重试	怎么推进
能力层	工具、模型、知识库	能做什么
数据层	记忆、日志、评估集	记得什么
治理层	权限、配额、审计	谁负责

缺治理层，规模越大越乱。参考 Hermes 团队的实践：每天处理 200+ 自动化任务，靠的是统一的调度与治理，而不是更聪明的模型。

二、五个共享能力

1. **模型网关**：统一鉴权、限流、计费与降级；
2. **工具注册表**：工具只登记一次，多个 Agent 复用；

3. **权限中心**：按角色授权，最小可用；
4. **审计日志**：谁、何时、调了什么、结果如何；
5. **配额管理**：按团队/任务设 token 与调用上限。

这五项不共享，每个 Agent 都会重复造轮子。

三、多租户隔离

- 数据隔离：不同部门的知识库与记忆分开；
- 权限隔离：工具按角色授权；
- 配额隔离：一个团队跑爆不影响其他人；
- 日志隔离：审计可按租户导出。

隔离不是“加个字段”，要在网关与数据层同时做。

四、上线路径

阶段	范围	标志
1	单团队、单流程	稳定运行 2 周
2	单部门、多流程	共享工具与日志
3	跨部门	网关、权限、配额上线
4	全公司	治理与审计常态化

不要跳阶段。第 2 阶段没跑稳就上第 3 阶段，问题会被放大。

五、30 分钟练习

1. 画五层结构（10 分钟）；
2. 列出你们最该共享的三项能力（5 分钟）；
3. 写四条多租户隔离要求（5 分钟）；
4. 标出当前处于哪个阶段（5 分钟）；
5. 写一条进入下一阶段的条件（5 分钟）。

六、验收清单

- [ ] 五层齐全，治理层有负责人；
- [ ] 模型网关统一鉴权限流；
- [ ] 工具登记可复用；
- [ ] 权限按角色最小化；
- [ ] 日志可按租户导出；
- [ ] 有分阶段上线条件。

七、延伸阅读

- 参考文章：基于 Hermes 打造企业级 Agent OS
- 知识库 `1.3 AI Agents（智能体）`
- 知识库 `4.3 团队搭建：AI 招聘/组队`

> 下一讲：多智能体编排。共享能力就绪后，才让多个 Agent 协作。
