

# 第 8 章 智能体搭建实操

所属模块：动手实践 · 第 7-9 章 建议学习时长：3 课时（含 2 课时实操，配代码资源）

## 学习目标

学完本章，你应该能够：

- 1. 使用低代码平台（以阿里云百炼为例）从零搭建一个业务智能体；
- 2. 为智能体配置角色提示词、知识库与工具调用；
- 3. 完成智能体的调试、发布与权限管理；
- 4. 理解 API 级开发的基本形态（附 Python 示例代码）。

## 正文

### 一、搭建智能体的两条路径

| 路径      | 适合人群        | 工具                                 |
|---------|-------------|------------------------------------|
| 低代码/可视化 | 业务骨干（本课程主力） | 阿里云百炼、Coze、钉钉 AI 助理                |
| 代码开发    | 技术学员/专业场景   | Python + OpenAI 兼容 SDK / LangChain |

本课程以低代码路径为主（第 8 章），代码路径提供示例供技术学员选学。

### 二、低代码搭建五步法（以百炼为例）

**第 1 步：创建智能体** 控制台 → 百炼 → 智能体应用 → 创建。命名清晰，如"报价助手-检测一部"。

**第 2 步：配置角色与指令** 把第 7 章的四要素提示词填进"系统提示词"：

"你是检测机构报价助手。依据价目表与折扣规则回答报价问题；信息不足时明确说明，不编造价格。"

**第 3 步：绑定知识库** 点击"添加知识库"，选择已建好的知识库（第 9 章会教搭建），让智能体回答时基于资料。

**第 4 步：配置工具** 按需开启工具：搜索引擎、代码解释器（计算）、或自定义 API（对接内部系统，如价目表接口、订单系统）。**这一步把智能体从"聊天"变成"办事"。**

**第 5 步：调试发布** 在调试窗口用真实问题测试 → 观察回答质量与工具调用记录 → 调整提示词 → 发布到渠道（网页链接、钉钉群机器人、API）。

### 三、调试技巧：看"思维过程"而非只看答案

低代码平台通常提供"运行日志"，能看到智能体每一步：模型怎么理解问题、调用了哪个工具、拿到了什么结果、最后怎么组织回答。  
大部分问题都能从日志里定位：

- 答非所问 → 检查系统提示词的角色与边界；
- 不用工具/乱用工具 → 检查工具描述是否清晰；
- 答错数字 → 检查是否接了计算工具、知识库是否最新；
- 答得太空 → 增加格式要求与示例。

## 四、发布与权限

发布前确认三件事：**访问渠道**（网页链接/群机器人/API）、**访问权限**（公开/内部/指定人）、**数据边界**（是否允许引用涉密知识库）。上线后设置监控：周使用量、失败率、用户反馈入口。

## 五、代码路径示例（技术学员选学）

百炼提供 OpenAI 兼容接口，代码模式与低代码模式可结合（见课程代码资源）：

```
import os
from openai import OpenAI

client = OpenAI(
    api_key=os.getenv("DASHSCOPE_API_KEY"), # 在阿里云百炼控制台获取
    base_url="https://dashscope.aliyuncs.com/compatible-mode/v1",
)

resp = client.chat.completions.create(
    model="qwen-plus",
    messages=[
        {"role": "system", "content": "你是一名企业知识库问答助手，回答须基于给定资料，不得编造。"},
        {"role": "user", "content": "请用一句话解释什么是 RAG（检索增强生成）。"},
    ],
)

print(resp.choices[0].message.content)
```

## 六、案例：制度问答智能体的迭代记录

某企业搭建"制度问答智能体"：v1 直接问答，准确率 60%；v2 绑定制度知识库 + 要求引用出处，准确率升至 85%；v3 增加"信息不足时明确说明"约束，并限制只回答制度范围问题，准确率 92%，"答非所问"显著减少。**每个版本都靠运行日志定位问题。**

### 关键概念小结

- 两条路径：低代码（业务骨干） / 代码（技术学员）
- 五步法：创建 → 指令 → 知识库 → 工具 → 调试发布
- 调试靠运行日志，看"思维过程"定位问题

- 发布前确认渠道、权限、数据边界

## 自测练习（对应作业 5）

1. 用低代码平台搭建一个业务智能体（报价/制度问答/巡检提醒任选）；
2. 配置角色提示词 + 至少 1 个工具；
3. 录制 3-5 分钟演示视频：说明场景、演示问答、展示运行日志优化过程。

## 融合吴恩达课程：对应模块

- **课程：**吴恩达《AI Agents》(DeepLearning.AI) —— 智能体底层机制（规划/记忆/工具/反思），帮助理解"为什么低代码平台这样设计"
- **链接：**<https://www.deeplearning.ai/short-courses/ai-agents/>
- **配套：**《Building Systems with the ChatGPT API》（系统化设计 LLM 应用，含多步流程编排）：  
<https://www.deeplearning.ai/short-courses/building-systems-with-chatgpt/>
- **进阶：**《LangChain for LLM Application Development》：<https://www.deeplearning.ai/short-courses/langchain-for-llm-application-development/>

技术学员建议按"Prompt 短课 → LangChain 短课 → AI Agents 短课"的顺序系统学完，即可具备从零开发智能体的能力。