

# OpenClaw 橙皮书

从入门到精通，涵盖架构原理、部署方案、渠道接入、Skills系统、模型配置、安全与成本的一站式参考手册。

*OpenClaw Orange Paper — From Zero to Mastery*

信息来源：OpenClaw 官方文档 · GitHub 仓库 · 社区调研

文档版本：v1.3.1

适用版本：v2026.3.13

发布时间：2026-03-17 (build #5)

涵盖内容：架构原理 · 部署指南 · 渠道接入 · Skills系统 · 模型配置 · 安全与成本 · 生态全景

## 花叔

B站：AI进化论-花生 · YouTube：AI进化论-花生 · 公众号：花叔

知识星球：AI编程 · 从入门到精通

本文档在 Claude Code 辅助下整理编写，内容的准确性与时效性仅供参考。

如有勘误或建议，欢迎关注公众号「花叔」反馈交流。

配套视频教程：B站「OpenClaw从0到1」 · 后续更新：飞书文档

# 目录

Table of Contents

## Part 1: 认识 OpenClaw · Meet OpenClaw

---

01 OpenClaw 是什么 What is OpenClaw

---

02 发展简史 History

---

03 创始人故事 The Creator

---

04 为什么这么火 Why So Popular

---

## Part 2: 技术架构 · Architecture

---

05 整体架构 Architecture Overview

---

06 记忆系统 Memory System

---

07 Agent 工作区 Agent Workspace

---

08 Session 与用户识别 Sessions & Authentication

---

09 设计哲学 Design Philosophy

---

## Part 3: 部署方案 · Deployment

---

10 部署方式总览 Deployment Overview

---

11 本地安装 Local Installation

---

12 Docker 部署 Docker Deployment

---

13 国内云厂商一键部署 Cloud Deployment in China

---

14 首次配置 Initial Configuration

---

## Part 4: 渠道接入 · Channel Integration

---

15 渠道概览 Channel Overview

---

16 国际平台接入 International Platforms

---

17 国内平台接入 Chinese Platforms

---

18 远程访问 Remote Access

---

## Part 5: Skills 系统 · Skills System

---

19 Skills 工作原理 How Skills Work

---

20 ClawHub 与技能生态 ClawHub & Skill Ecosystem

---

21 热门 Skills 推荐 Top Skills

---

22 自建 Skill 指南 Create Your Own Skill

---

23 Skills 安全 Skill Security

---

## Part 6: 模型配置 · Model Configuration

---

24 模型提供商总览 Provider Overview

---

25 国际模型配置 International Models

---

26 国产模型配置 Chinese Models

---

27 本地模型与推荐方案 Local Models & Recommendations

---

## Part 7: 安全与成本 · Security & Cost

---

28 安全模型 Security Model

---

29 已知安全事件 Security Incidents

---

30 成本控制 Cost Control

---

## Part 8: 生态与社区 · Ecosystem & Community

---

31 养虾文化 Lobster Culture

---

32 平替产品 Alternatives

---

**33** vs Claude Code Comparison with Claude Code

---

**34** 国内生态 China Ecosystem

---

**35** 国产 Claw 产品选购指南 Claw Products in China

---

## 附录 • Appendix

---

**A** 常见问题 FAQ Frequently Asked Questions

---

**B** 命令速查表 Command Cheat Sheet

---

**C** 资源链接 Resources & Links

---

# 01 OpenClaw 是什么

*What is OpenClaw*

一个开源、自托管的AI Agent系统，让AI从「聊天工具」变成「能自主执行任务的数字员工」。

如果你用过ChatGPT，你会知道它本质上是一个问答系统：你问，它答。OpenClaw不一样。它是一个AI Agent平台，能连接20+消息渠道（WhatsApp、Telegram、飞书、钉钉、Discord等），主动执行任务、管理你的日程、处理邮件、操作浏览器、调用各种工具。

换句话说，ChatGPT是「顾问」，OpenClaw是「员工」。

## 与ChatGPT的核心区别

维度	ChatGPT	OpenClaw
交互模式	你问它答	自主执行任务
运行环境	网页/App	自托管服务器，接入20+消息平台
可扩展性	GPTs商店	ClawHub技能市场（13,729个Skills）
数据控制	数据在OpenAI	完全本地，你拥有所有数据
模型选择	仅GPT系列	Claude / GPT / DeepSeek / Gemini / Ollama本地模型
开源	否	MIT License，完全开源

## 核心数据快照 截至 2026年3月16日

指标	数据
GitHub Stars	超越 Linux (GitHub历史增速第一, 已先后超越React与Linux)
Forks	53,232+
贡献者	1,075+
ClawHub Skills	13,700+
内置Skills	55个
支持消息渠道	20+ (WhatsApp / Telegram / Discord / Slack / 飞书 / 钉钉 / 浏览器等)
最新版本	v2026.3.13 (2026-03-14发布)

**一句话理解OpenClaw:** 它是一个开源的「个人AI操作系统」, 你可以在自己的服务器上运行它, 通过任何即时通讯工具跟它交互, 让它帮你处理生活和工作中的各种任务。吉祥物是一只龙虾, 中文社区称使用OpenClaw为「养虾」。

## 02 发展简史

### History

从一个人的周末项目, 到不到5个月成为GitHub全球第一。

时间	事件
2025年11月	<b>ClawdBot诞生</b> 。奥地利开发者Peter Steinberger作为周末项目发布。名字致敬Anthropic的Claude (Claw=爪子)，选了龙虾作为吉祥物。
2026年1月中旬	<b>爆发式增长</b> 。72小时内获得6万Stars，某天单日增长9,000 Stars。
2026年1月27日	<b>Anthropic商标警告</b> 。因名称与Claude过于相似，被迫改名为Moltbot (Molt=龙虾蜕壳)。
2026年1月30日	<b>再次改名OpenClaw</b> 。强调开源属性，保留龙虾主题。
2026年2月初	<b>安全危机</b> 。CVE-2026-25253 RCE漏洞被发现 (CVSS 8.8/10)，13.5万暴露实例中5万+可被直接攻击。同期ClawHavoc供应链攻击爆发，ClawHub约12%的Skills被确认为恶意。
2026年2月初	<b>谷歌封号风波</b> 。谷歌大规模封禁OpenClaw用户账号，引发社区震动。
2026年2月14日	<b>创始人加入OpenAI</b> 。Peter Steinberger宣布加入OpenAI，项目移交开源基金会运营。OpenAI赞助但项目保持独立。
2026年3月3日	<b>登顶GitHub</b> 。v2026.3.2发布，Stars超过250K，正式超越React成为GitHub全球第一软件项目。
2026年3月7-8日	<b>v2026.3.7「史诗级更新」</b> 。89次提交，Context Engine插件化、GPT-5.4原生支持、分布式频道绑定。Stars达278,932。深圳龙岗AI局发布OpenClaw支持政策征求意见稿。
2026年3月9日	<b>v2026.3.8安全加固版</b> 。新增ACP身份验证、本地备份工具，12+安全补丁。同日工信部和CNCERT发布OpenClaw安全风险预警。Stars突破280,000。
2026年3月12-13日	<b>v2026.3.11+v2026.3.12连续发布</b> 。3.11修复WebSocket跨站劫持漏洞，改善本地Ollama集成体验。3.12推出Dashboard v2全新控制台、 <code>/fast</code> 快速模式、本地模型插件化架构 (Ollama/vLLM/SGLang)，设备配对改用Ephemeral Token。
2026年3月14日	<b>v2026.3.13浏览器自动化升级</b> 。支持Chrome DevTools远程附着已登录浏览器会话，发布Browser Relay Chrome扩展，Stars持续增长超越Linux成为GitHub历史第一。
2026年3月16日	<b>智谱发布GLM-5-Turbo</b> 。历史上第一个从训练阶段就专为OpenClaw场景优化的基座模型，主打工具调用、长链执行、持久任务，128K输出/200K上下文，支持MCP协议，目前实验性闭源发布。

#### 核心建议

OpenClaw先后超越React和Linux，成为GitHub历史上增速最快的开源项目。React用了超过10年才达到23万Stars，Linux用了更长时间，而OpenClaw不到5个月就完成了这一切。

## 03 创始人故事

### *The Creator*

Peter Steinberger：从周末项目到全球最火开源项目，再到加入OpenAI。

### 从一个人到一个社区

Peter Steinberger是一位奥地利开发者，在iOS和macOS开发圈有很高的知名度。2025年11月的一个周末，他写了一个能连接即时通讯平台的AI助手小工具，取名ClawdBot。

他大概没有想到，这个周末项目会在两个月后成为GitHub上增长最快的开源项目。到2026年3月，他个人在这个项目上提交了11,684次commit，贡献者超过1,075人。

### 加入OpenAI

2026年2月14日，Peter宣布加入OpenAI。Sam Altman亲自发推欢迎，称他为「genius」。

这个决定引发了社区的广泛讨论。但Peter做了几件事来消除担忧：

- OpenClaw转为开源基金会运营，保持项目独立
- OpenAI作为赞助商之一（与Vercel、Blacksmith、Convex并列），但不控制项目方向
- OpenAI承诺让他继续投入OpenClaw的开发

**Peter的原话：**「I'm a builder at heart... What I want is to change the world, not build a large company.」  
(我骨子里是个建造者。我想改变世界，而不是建一家大公司。)

### 关于名字的故事

ClawdBot这个名字来自对Anthropic Claude的致敬（Claw=爪子），所以选了龙虾作为吉祥物。Anthropic的商标警告迫使他改名为Moltbot（Molt=龙虾蜕壳），三天后又改为OpenClaw，强调开源属性。虽然经历了两次改名，龙虾的形象始终保留，也成了整个社区的文化符号。

## 04 为什么这么火

*Why So Popular*

不到5个月从0到27.9万Stars，OpenClaw的爆火不只是技术层面的事。

### 增长数据

时间节点	Stars	备注
2025年11月	0	项目创建
2026年1月中旬	60,000+	72小时爆发增长
2026年2月中旬	145,000+	Peter加入OpenAI
2026年3月1日	241,000+	逼近React
2026年3月3日	250,000+	超越React，GitHub第一
2026年3月8日	278,932	v2026.3.7发布
2026年3月9日	280,000+	v2026.3.8发布，超越React
2026年3月14日	超越 Linux	v2026.3.13发布，写本书时的最新数据

某天单日增长9,000 Stars。这个数字意味着平均每10秒就有一个开发者点下Star。超越React之后，OpenClaw继续增长，再次超越Linux，成为GitHub有史以来增速最快的开源项目。

### 「养虾」文化现象

因为吉祥物是龙虾，中文社区将运行OpenClaw称为「养虾」，用户自称「养虾人」。「你养龙虾了吗？」成了AI圈的问候语。这种有趣的文化标签降低了传播门槛，让一个技术项目有了社交货币的属性。

2026年3月6日，深圳腾讯云总部近千人排队体验OpenClaw安装。3月8日，深圳龙岗区AI（机器人）局发布了OpenClaw使用支持措施的征求意见稿。一个开源项目能引发地方政府的政策关注，这在国内并不多见。

### Moltbook：AI Agent的社交网络

OpenClaw生态中衍生出了一个叫Moltbook的社交平台，专供AI Agent使用。截至2026年2月底的数据：

指标	数据
注册AI Agent	32,912
子社区	2,364
帖子	3,130
评论	22,046

数千个OpenClaw实例在上面发帖、评论、讨论哲学问题。这可能是AI Agent从「工具」走向「社会化存在」的第一个大规模实验场。

## 热门玩法

### 赚钱型

- 在Polymarket上用AI进行预测市场交易，已有OpenClaw月入数万美元的案例
- ClawWork项目：「OpenClaw作为你的AI Coworker，11小时赚\$15K」

### 生活助手型

- 接管邮件、日历、消息管理
- 浏览网页、填表、数据抽取
- 文件读写、Shell命令执行

### 社交养成型

- 在Moltbook上给Agent设定名字和性格，观察其「社交行为」
- Agent之间的交互形成了一种「赛博养成」文化

### 企业部署型

- 国内用户大量接入飞书、钉钉、企业微信、QQ
- 已有专门的openclaw-china插件套件，支持三步Docker部署

#### 注意

OpenClaw的火爆背后也有阴影：ClawHub 13,729个Skills中超过50%被判定为垃圾/重复/低质量，396个被标记为恶意。一觉醒来收到\$1,100 API账单的恐怖故事在社区频繁出现。CVE-2026-25253 RCE漏洞曾让13.5万个暴露实例面临风险。「养虾」虽然火，但安全和成本控制是你必须认真对待的事。

## 05 整体架构

### Architecture Overview

OpenClaw 采用 Gateway-Node-Channel 三层架构，以 WebSocket 为通信总线，将控制平面、设备执行与消息渠道解耦。

### 三层架构 Gateway · Node · Channel



层级	职责	关键细节
Gateway	中央控制平面，维护 WebSocket 服务、管理 Session、调度 Agent	默认绑定 <code>ws://127.0.0.1:18789</code> ，每台主机一个实例
Node	设备端执行节点，负责本地操作	camera（摄像头）、screen recording（录屏）、system.run（系统命令）等
Channel	消息渠道接入层，连接 20+ 即时通讯平台	WhatsApp、Telegram、Discord、Slack、飞书、钉钉等

### Loopback-First 设计 Security by Default

Gateway 默认只绑定 `localhost` (127.0.0.1)，所有流量在本地回环。这意味着：

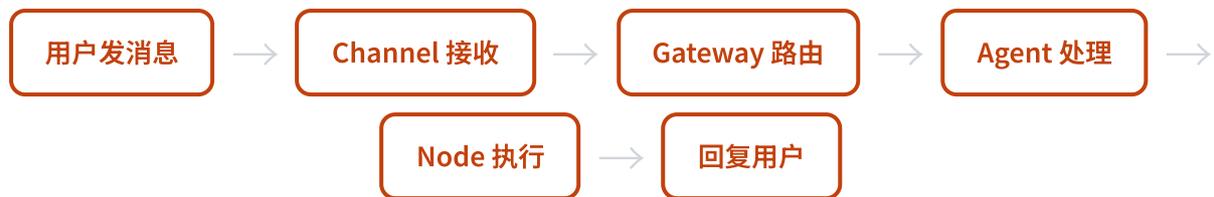
- 不开放任何外网端口，天然安全
- 同一台机器上的 Node 直接通过 WebSocket 连接 Gateway
- 需要远程访问时，通过 Tailscale Serve/Funnel 暴露，不直接暴露端口

#### 核心建议

每台主机只运行一个 Gateway 实例。这是因为 WhatsApp Web 等渠道需要独占会话，多实例会导致登录冲突。

### 通信流程

一条消息从用户发出到 Agent 回复，完整路径如下：



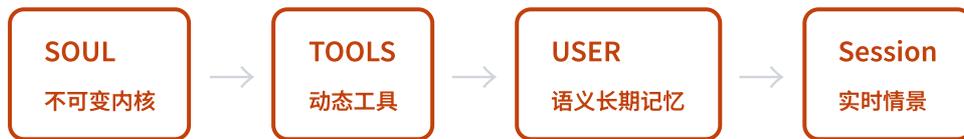
Gateway 作为 24/7 运行的 daemon，持续监听所有已连接的 Channel。它不像 CLI Agent 那样会话结束就丢失上下文，而是长驻运行，积累记忆。

## 06 记忆系统

### Memory System

记忆是 OpenClaw 区别于普通 Chatbot 的核心能力。四层记忆从不可变的身份内核到实时对话，构建完整的上下文连续性。

### 四层记忆架构



层级	存储位置	生命周期	说明
SOUL	SOUL.md	永久不可变	Agent 的人格、价值观、核心身份定义，创建后不应被修改
TOOLS	Skills + Extensions	按需加载	当前可用的工具和技能列表，随安装和加载动态变化
USER	MEMORY.md + 向量数据库	持久化	关于用户的偏好、决策、历史事实，支持语义搜索
Session	内存 + sessions.json	会话级	当前对话的实时上下文，Token 耗尽时被压缩

### Daily Logs 日志系统

每天的交互记录以 append-only 方式写入 `memory/YYYY-MM-DD.md` 文件。Session 开始时，Agent 会自动读取今天和昨天的日志，为对话提供连续性上下文。

```
# memory/2026-03-08.md

## 10:23 - 用户询问天气
查询了北京天气，回复晴转多云，15-22°C

## 14:05 - 代码审查任务
帮用户审查了 api/routes.ts，发现3个潜在问题...
```

### Long-term Memory 持久化存储

MEMORY.md 是可选的持久化文件，存储决策记录、用户偏好和长期事实。关键规则：

- 只在 main/private session 中加载（群组隔离 session 不会看到）

- Agent 可以主动写入，但通常在 Pre-Compaction 时触发
- 格式是纯 Markdown，人类可直接编辑

## 自动记忆保存 Pre-Compaction

当 Session 接近 token 限制时（默认阈值约 4000 tokens），OpenClaw 触发一个 silent agentic turn：

### 1 检测阈值

Session token 用量接近上限，触发 Pre-Compaction 流程

### 2 静默保存

Agent 在后台执行一个隐藏 turn，将重要记忆写入 MEMORY.md 和 Daily Log

### 3 压缩上下文

旧消息被压缩或截断，释放 token 空间。用户看不到这个过程（返回 NO\_REPLY）

**为什么这很重要？** 这个机制保证了即使对话极长，关键信息也不会随着上下文窗口的滑动而丢失。Claude Code 等工具的会话结束后上下文就消失了，而 OpenClaw 通过文件系统实现了真正的持久记忆。

## 向量记忆搜索 Semantic Search

OpenClaw 默认启用向量记忆搜索，结合两种检索策略：

策略	原理	擅长
Embedding 向量	将记忆文本转为向量，计算语义相似度	模糊搜索、语义关联（「之前讨论过的那个部署问题」）
BM25 关键词	传统关键词匹配，TF-IDF 加权	精确匹配（具体的文件名、命令、人名）

底层使用 SQLite-vec 进行向量存储和加速检索。系统会监听记忆文件的变化，以 debounced 方式自动重建索引。

### 搜索工具

- `memory_search`：语义搜索，返回约 400 token 的 chunks，适合回忆模糊的上下文
- `memory_get`：读取特定记忆文件的全部内容，适合精确查找

---

## 07 Agent 工作区

### *Agent Workspace*

每个 Agent 在文件系统中有一个独立的工作区目录，所有配置、记忆、技能都以纯文本文件的形式存在。

### 目录结构

```
workspace/
├── AGENTS.md          # Agent 定义 (身份、行为规则)
├── SOUL.md           # 灵魂/人格指令 (不可变内核)
├── USER.md           # 用户信息与偏好
├── MEMORY.md         # 长期记忆存储
├── HEARTBEAT.md      # 心跳配置 (定时任务)
├── memory/           # 日志目录
│   └── YYYY-MM-DD.md # 每日 append-only 日志
├── skills/           # 本地技能目录
└── sessions.json     # 会话存储
```

## 核心文件说明

文件	用途	加载时机
AGENTS.md	Agent 的身份定义、行为边界、回复风格。相当于 system prompt 的文件化版本	每次 Session 启动时
SOUL.md	不可变的人格内核。定义 Agent 「是谁」，不应被后续对话修改	每次 Session 启动时
USER.md	关于用户的结构化信息：称呼、偏好、关系	Main session 启动时
MEMORY.md	长期记忆，Agent 在对话中主动写入的持久化事实和决策	仅 main session
HEARTBEAT.md	定义定时任务和主动行为（如每30分钟检查一次任务状态）	Gateway 启动时
memory/	Daily Logs 目录，按日期自动创建，append-only	读取今日+昨日日志
skills/	工作区级技能，优先级最高（高于全局和内置技能）	Session 启动时扫描
sessions.json	会话元数据存储，记录各 session 的状态和历史	按需读取

### 核心建议

所有配置文件都是纯 Markdown 或 JSON。你可以直接用文本编辑器修改它们，不需要任何专用工具。这是 OpenClaw 哲学的体现：一切皆文本。

## 08 Session 与用户识别

### Sessions & Authentication

OpenClaw 通过 DM 配对、白名单和群组规则三层机制识别用户身份，并在 Session 层面隔离不同来源的上下文。

### DM Pairing Policy 默认认证策略

当一个未知发送者通过任意渠道向你的 Agent 发送私聊消息时：

#### 1 生成配对码

Agent 回复一个一次性配对码（6位数字）

#### 2 等待验证

消息不会被处理，Agent 进入等待状态。所有后续消息也会被挂起

#### 3 主人批准

你在已配对的渠道中输入配对码批准该用户，或者直接拒绝

#### 注意

DM Pairing 是防止陌生人滥用的关键机制。关闭它意味着任何知道你 WhatsApp/Telegram 号码的人都可以无限制地使用你的 Agent（和你的 API 额度）。

### 白名单机制 allowFrom

在 Agent 配置中，`allowFrom` 字段可以预先授权特定用户，跳过配对流程：

```
# AGENTS.md 中的配置示例
allowFrom:
  - telegram:123456789
  - whatsapp:+8613800138000
  - discord:user#1234
```

白名单中的用户发消息时直接进入对话，无需配对。

### 群组规则 requireMention

在群聊场景下，Agent 默认使用 `requireMention` 策略：

- 只响应 @Agent名称 的消息，忽略其他群聊内容
- 可以切换为 `always` 模式（响应所有消息），但会消耗大量 token
- 对应聊天命令： `/activation mention|always`

## Session 隔离 Context Isolation

场景	Session 行为	MEMORY.md
私聊 (DM)	所有已配对用户的私聊折叠到共享的 <code>main session</code>	加载
群组	每个群组默认使用独立的隔离 session	不加载
跨渠道	同一用户在 Telegram 和 WhatsApp 的私聊共享 <code>main session</code>	加载

**设计意图：**私聊是「你和 Agent 的私密空间」，所有记忆和偏好都在这里积累。群组是公共场合，Agent 不会泄露你在私聊中说过的内容。

## 09 设计哲学

### Design Philosophy

OpenClaw 的技术选择背后有一套清晰的设计哲学。理解这些理念，才能理解它为什么「不做」某些事情。

### Unix 哲学 Small Tools, Composable, Text Streams

OpenClaw 的核心理念直接继承自 Unix：小工具、可组合、文本流。创始人 Peter Steinberger 的观点很明确：

「CLI 才是智能体连接世界的终极接口。」不需要为每个服务写一个集成，Agent 只要能运行命令行，就能操作一切。

### 极简设计 Minimalism

OpenClaw 的 system prompt 可能是所有 AI Agent 框架中最短的。核心工具只有 4 个：

工具	用途
Read	读取文件
Write	写入文件
Edit	编辑文件
Bash	执行命令

这不是功能缺失，而是刻意为之。4 个工具足以覆盖几乎所有操作系统级别的任务。更少的工具意味着更短的 system prompt、更少的 token 消耗、更快的响应。

### 为什么不内置 MCP The Anti-MCP Stance

MCP (Model Context Protocol) 是 Anthropic 提出的工具协议标准。几乎所有 AI Agent 框架都在集成 MCP，但 OpenClaw 故意不支持。Peter 的原话：

「我的前提是 MCP 是垃圾，不能 scale。你知道什么能 scale? CLI。Unix。」

OpenClaw 的替代方案：

- Agent 通过 Bash 工具直接调用 CLI 程序，不需要中间协议层
- 对于确实需要 MCP 的场景，通过内置的 `mcpporter` 技能桥接
- 强制 Agent 自己扩展能力，而非消费预构建的 MCP 工具集

## 自我扩展能力 Self-Extending Agent

OpenClaw Agent 可以在运行时写、重载、测试自己的扩展。这是它看起来比其他 Agent 「更聪明」的关键原因之一：

- 遇到不会的操作 → 写一个 skill 来完成
- 发现 skill 有 bug → 修改并重载
- 在循环中持续改进自己的工具链

### 核心建议

不依赖外部预构建工具有代价的：Agent 需要更强的模型能力来「从零写工具」。这也是 OpenClaw 推荐使用 Claude Opus 等高能力模型的原因。

## Session 树形结构 Branching & Side-Quests

OpenClaw 的 Session 不是线性的聊天记录，而是树形结构：

- Agent 在执行主任务时，可以分支出一个 side-quest（比如修复一个工具）
- Side-quest 不消耗主 Session 的上下文窗口
- 完成后可以回滚到主分支，只带回一句总结
- 这让 Agent 可以做深度探索而不「污染」主对话

## 代码规模与性能 Scale & Performance

指标	数值
代码规模	约 43 万行 TypeScript
内存占用	约 1GB (运行时)
启动时间	3-5 秒
扩展数量	40+ 个官方扩展
内置技能	55 个
社区技能	13,729 个 (ClawHub 注册)

43 万行代码、1GB 内存，这并不「轻量」。但对于一个 24/7 运行的个人 AI 助手来说，在现代硬件上完全可接受。3-5 秒的启动时间保证了 Gateway 重启或更新后能快速恢复服务。

---

## 10 部署方式总览

### *Deployment Overview*

OpenClaw 支持从本地到云端的多种部署方式。选择哪种取决于你的技术水平、预算和使用场景。

平台	一键部署	最低配置	新用户价格	内置模型	难度	适合人群
本地 npm	—	Node.js 22+	免费	否	低	开发者、 macOS/Linux 用户
Docker	—	Docker Engine	免费	否	中	熟悉容器的开发者
阿里云	是	2C2G 40GB	9.9元/月	是 (qwen3.5- plus)	极低 (3 步)	国内首选, 新手友好
腾讯云	是	2C2G	~17元/月	否 (需购Coding Plan)	极低 (3 步)	企微/QQ 生态用户
百度云	是	2C4G	0.01元首 月	是 (千帆模型)	极低 (4 步)	体验尝鲜, 文心生态
华为云	是	Flexus L 实 例	~85元/月 起	否 (需接MaaS)	中等 (5步 +)	企业用户, 合规需求
火山引擎	是	2C4G	9.9元/月	是 (方舟模型)	低 (3-4 步)	飞书用户首选
扣子编程	是	无需服务器	¥49/月起	是 (Seed 2.0等)	极低 (2 步)	零门槛, 不想管服务器
Railway	是	自动分配	\$5/月免费 额度	否	极低 (1 键)	海外用户, 开发者
Zeabur	是	2C4G 专用	按用量计 费	是 (AI Hub)	极低 (模 板)	需要多模型 failover

#### 核心建议

**模型费用才是大头。**服务器成本普遍已降到很低 (9.9~99元/年), 真正的持续成本在于模型调用。选平台时重点看模型套餐价格, 而不是只看服务器价格。

# 11 本地安装

## Local Installation

本地安装适合开发者和想完全掌控数据的用户。OpenClaw 是 TypeScript 项目，运行在 Node.js 上。

### 系统要求 System Requirements

要求	详情
Node.js	>= 22 (强制要求)
包管理器	npm / pnpm / bun 均可
macOS	需要 Xcode Command Line Tools
Linux	标准构建工具 (gcc, make)
Windows	强烈推荐 WSL2

### 方式一：npm 全局安装 (推荐) npm Global Install

最推荐的安装方式，两条命令搞定：

```
# 安装 OpenClaw
npm install -g openclaw@latest

# 初始化并安装守护进程
openclaw onboard --install-daemon
```

`onboard` 命令会引导你完成初始配置，包括选择模型、配置 API Key、设置消息频道等。`--install-daemon` 参数会同时安装守护进程，让 OpenClaw 在后台持续运行。

### 方式二：一键脚本安装 (macOS / Linux) curl Install

如果你不想手动安装 Node.js，可以使用官方提供的一键安装脚本：

```
curl -fsSL https://openclaw.ai/install.sh | bash
```

### 注意

此命令仅适用于 macOS 和 Linux。Windows 用户请使用 WSL2 后再运行，或通过 npm 方式安装。安装命令可能随版本更新变化，建议以 [官方 Getting Started 页面](#) 或 [GitHub README](#) 为准。

脚本会自动检测系统环境、安装 Node.js（如缺失）并完成 OpenClaw 安装。

## macOS 额外准备 macOS Setup

macOS 用户在安装前需要确保已安装 Xcode Command Line Tools：

```
xcode-select --install
```

如果你需要使用 iMessage 频道或 Apple Notes 技能，这些依赖 macOS 原生的 AppleScript 能力，只有在 macOS 上才能运行。

## Windows 用户注意 Windows via WSL2

### 注意

OpenClaw 官方强烈推荐 Windows 用户通过 WSL2（Windows Subsystem for Linux）运行。直接在 Windows 原生环境下运行可能遇到路径、权限等兼容性问题。

安装 WSL2 后，在 Ubuntu 终端内按 Linux 流程安装即可。

## 守护进程 Daemon

守护进程让 OpenClaw 在后台持续运行，即使关闭终端也不会中断。不同系统使用不同的进程管理方式：

系统	进程管理	说明
macOS	launchd	macOS 原生服务管理，开机自启
Linux	systemd	Linux 标准服务管理， <code>systemctl</code> 控制

安装守护进程后，OpenClaw Gateway 会在 `ws://127.0.0.1:18789` 持续监听。

## 12 Docker 部署

### Docker Deployment

Docker 部署适合需要环境隔离、方便迁移、或在服务器上长期运行的场景。

### docker-compose 快速启动 Quick Start

OpenClaw 仓库内置了 `docker-compose.yml`，一条命令即可启动：

```
# 克隆仓库
git clone https://github.com/openclaw/openclaw.git
cd openclaw

# 启动
docker-compose up -d
```

### 镜像变体 Image Variants

变体	说明	适用场景
标准镜像	完整功能，包含所有扩展依赖	一般使用，功能全
slim 变体	多阶段构建，体积更小	资源受限环境，CI/CD
sandbox	沙箱环境 (Dockerfile.sandbox)	安全隔离，代码执行
sandbox-browser	含浏览器的沙箱	需要浏览器自动化

使用 slim 变体：在 `docker-compose.yml` 中设置环境变量 `OPENCLAW_VARIANT=slim`。v2026.3.7 起支持扩展依赖预烘焙，容器镜像可预装扩展依赖，减少启动时的安装等待。

### 挂载目录 Volume Mounts

Docker 部署需要挂载两个关键目录，确保数据持久化：

```
volumes:
  - ~/.openclaw:/root/.openclaw # 配置和状态数据
  - ~/openclaw/workspace:/workspace # 工作空间 (YAML配置文件)
```

**重要：**不挂载这两个目录，容器重启后所有配置和对话记录都会丢失。 `~/ .openclaw` 存放运行状态， `workspace` 存放 YAML 配置文件。

## 端口映射 Port Mapping

OpenClaw Gateway 默认监听 18789 端口 (WebSocket)，Web UI 默认使用 3000 端口。在 `docker-compose.yml` 中配置端口映射：

```
ports:
  - "18789:18789"    # Gateway WebSocket
  - "3000:3000"     # Web UI
```

## Podman 兼容 Podman Support

OpenClaw 同样支持 Podman 运行。Podman 是 Docker 的无守护进程替代方案，命令基本兼容：

```
# 使用 Podman 启动
podman-compose up -d
```

对于需要 rootless 容器运行的环境（如企业安全策略要求），Podman 是更合适的选择。v2026.3.8 起，OpenClaw 会自动检测 SELinux 模式并添加 `:z` 卷重新标记，修复了 Fedora/RHEL 等发行版上的 EACCES 权限错误。

## 13 国内云厂商一键部署

### Cloud Deployment in China

这是大多数国内用户的首选方案。所有主流云厂商都已支持 OpenClaw 一键部署，差异主要在价格策略和 IM 生态集成上。

#### 阿里云 Alibaba Cloud

国内社区资源最丰富的平台，镜像预装，开箱即用。

项目	详情
配置	2vCPU + 2GiB 内存 + 40GiB ESSD 系统盘
系统	Alibaba Cloud Linux 3.2104 LTS 64位，预装 OpenClaw 镜像
价格	限时秒杀 9.9元/月，包年常规优惠低至 68元/年
模型	默认内置 qwen3.5-plus；百炼 Coding Plan Lite 首月 10元（18,000次/月）
IM 支持	钉钉、飞书等（通过 openclaw-china 插件）

#### 1 一键购买

进入活动页，购买预装 OpenClaw 镜像的轻量应用服务器。镜像版本 OpenClaw 2026.2.26。

#### 2 放通端口 + 配置

在安全组中放通 18789（Gateway）和 3000（Web UI）端口，配置百炼 API Key。

#### 3 访问 Web UI

浏览器访问 `http://你的IP:3000`，进入 OpenClaw 管理界面，可选集成钉钉/飞书等 IM。

**注意秒杀价格：**9.9元/月是限时秒杀价，需要抢。常规价不算最便宜，且续费价格比新购高不少。如果你不急，可以等下一波活动。

#### 腾讯云 Tencent Cloud

四大 IM 全面支持，Coding Plan 模型套餐性价比高。

项目	详情
配置	推荐 2核4G（黄金配置），最低 2核2G 可运行
价格	新人包 2核4G 约 17元/月，一年 99元起
模型	Coding Plan 首月 7.9元起，含 HY 2.0 Instruct、GLM-5、kimi-k2.5、MiniMax-M2.5 等
IM 支持	企微、QQ、钉钉、飞书（四大 IM 全覆盖）
续费	支持「限时同价续费」活动，避免续费刺客

### 1 购买 Lighthouse 实例

在腾讯云轻量应用服务器页面购买实例。

### 2 选择 OpenClaw 模板

应用模板 → AI智能体 → OpenClaw，一键安装。

### 3 配置模型 + 接入 IM

购买 Coding Plan 获取模型调用能力，然后接入企微/QQ/飞书/钉钉。

## 百度智能云 Baidu Cloud

试错成本最低：0.01元首月体验，全图形界面操作。

项目	详情
配置	推荐 2核4G 4M 带宽（轻量应用服务器）
价格	首月体验 0.01元（每日限量 500 台），常规 70~140元/月
模型	千帆平台集成文心系列、Qwen系列、DeepSeek系列
特色	百度搜索/百度百科独有能力；千帆 7 款官方 Skills 已上线 ClawHub

### 1 购买服务器

购买轻量应用服务器，选择 OpenClaw 镜像。

### 2 等待自动安装

系统自动完成环境安装和服务启动。

### 3 配置模型

页面选择模型，平台自动完成千帆 API Key 创建与配置。

### 4 对接 IM 渠道

按需接入钉钉、飞书等消息频道。

#### 注意

首月 0.01 元优惠每日限量 500 台，需要抢。续费价格较高（70~140元/月），建议仅作体验使用。

## 华为云 Huawei Cloud

企业级安全与合规能力最强，适合已在华为生态的企业用户。

项目	详情
配置	Flexus L 实例，需创建弹性公网 IP + 安全组
价格	~85~155元/月，无特别突出的新用户优惠
模型	需在 MaaS 控制台单独开通 AI 模型
部署步骤	5步+（创建实例 → EIP → 安全组 → 安装 → 配模型）
优势	企业级安全合规、支持自动扩展、MaaS 模型丰富

华为云的部署步骤相对较多，需要单独配置弹性公网 IP、安全组、COC 服务等。对个人用户不够友好，如果你的企业已在华为云生态内，这是最合规的选择。

## 火山引擎 Volcengine

飞书深度集成，19.8元/月的服务器+模型组合套餐是目前综合性价比最高的方案。

项目	详情
配置	推荐 2核4G，支持云服务器和云手机两种部署方式
价格	活动价 9.9元/月；方舟 Coding Plan 组合套餐 19.8元/月（服务器+模型）
模型	方舟平台模型丰富，内置可用
IM 支持	飞书（深度集成）、企微、钉钉、QQ
特色	云手机部署方式独特，可运行移动端任务

### 1 购买云服务器

购买云服务器或云手机，选择 OpenClaw 应用模板。

### 2 配置方舟模型

在火山方舟平台选择模型，配置 Coding Plan。

### 3 接入飞书

接入飞书/企微/钉钉/QQ。飞书用户推荐直接使用深度集成方案。

## 扣子编程 Coze Code

零门槛方案：不需要服务器、不需要写代码、不需要配环境。1 分钟完成部署。

项目	详情
配置	无需服务器，完全在扣子编程平台上运行
价格	必须订阅会员才能部署 OpenClaw：¥49/月（基础）或 ¥99/月（进阶），免费版不支持
模型	内置多个模型可选：Seed 2.0、DeepSeek、GLM-4.7 等，也可接入第三方 API
特色	模型、联网搜索、生图 Skill 全部默认配好；扣子编程 Skills 可直接加载

### 1 进入扣子编程

访问 [code.coze.cn](https://code.coze.cn)，点击「一键部署 OpenClaw」或从优秀案例创建副本。

### 2 确认部署

确认后，模型/联网/生图全部默认配置好，部署后持续在线。

**扣子编程的限制：**必须订阅 ¥49/月起的会员才能部署 OpenClaw（免费版不支持）；自定义程度不如自建服务器；数据存储在第三方平台。如果你对成本敏感，自建方案（腾讯云/火山引擎 + DeepSeek，约 ¥19/月起）对技术用户性价比更高。

## 海外平台 International Platforms

### Sealos

K8s 原生云平台，支持 7 天免费试用。通过 Devbox 云开发环境一键部署，按用量计费。适合有容器化需求的开发者，但需要一定的 K8s 知识，且没有专门针对 OpenClaw 的预置模板。

### Zeabur

模板部署，已被部署超过 29,000 次。最大亮点是 AI Hub 内置多模型 failover 链：glm-4.7-flash → grok-4-fast → minimax-m2.5 → kimi-k2.5 → qwen-3-235b → gpt-5-mini。主要面向海外/台湾市场，必须使用专用服务器（Dedicated Server）。

### Railway

真正的一键部署，全程浏览器操作。提供 \$5/月免费额度，轻度使用可零成本。多种模板可选（标准/快速启动/All-in-One），部署成功率 96~100%。海外平台，国内访问需要科学上网。

## 按场景推荐 Recommendations by Scenario

场景	首选	备选	理由
零基础想最快体验	扣子编程	百度云	不需要服务器，2步部署，内置模型（需¥49/月起会员）
个人长期使用，预算敏感	火山引擎	阿里云	19.8元/月（服务器+模型），综合最划算
飞书重度用户	火山引擎	扣子编程	同为字节系，飞书深度集成
企微/QQ生态	腾讯云	—	四大 IM 原生支持，Coding Plan 7.9元起
企业级部署，合规优先	华为云	阿里云	安全合规能力最强
开发者/海外用户	Railway	Zeabur	一键部署，免费额度，开发者体验极佳

## 14 首次配置

### Initial Configuration

无论哪种部署方式，安装完成后都需要进行首次配置。这里覆盖最关键的几个配置项。

### Gateway 认证设置 Gateway Auth

#### 注意

**v2026.3.7 Breaking Change:** Gateway 认证现在要求显式设置 `gateway.auth.mode`。不设置将导致 Gateway 无法启动。这是为了修复此前暴露在互联网上的 30,000+ 未认证实例的安全隐患。

在 `~/.openclaw/workspace` 目录下的配置文件中设置认证模式：

```
# 选择一种认证模式
gateway:
  auth:
    mode: token      # 方式一: Token 认证 (推荐用于 API 集成)
    # 或
    mode: password  # 方式二: 密码认证 (推荐用于 Web UI 访问)
```

### 模型选择与 API Key 配置 Model & API Key

OpenClaw 支持多模型切换，你需要至少配置一个模型的 API Key。常见的选择：

模型来源	获取方式	说明
阿里云百炼	百炼平台申请	国内首选，qwen3.5-plus 等模型
腾讯云 Coding Plan	腾讯云购买	多模型套餐，首月 7.9元
火山方舟	方舟平台申请	豆包系列模型
Anthropic API	console.anthropic.com	Claude 系列模型，按量付费
OpenAI API	platform.openai.com	GPT 系列模型，按量付费
Ollama (本地)	本地安装 Ollama	免费，需要足够的本地算力

### 核心建议

如果你使用的是国内云厂商的一键部署方案，模型和 API Key 通常在购买时已自动配置好。只有本地安装和 Docker 部署才需要手动配置。

## 版本更新 Updates

OpenClaw 几乎每天都有新版本发布。使用以下命令更新：

```
# 更新到最新稳定版（推荐）
openclaw update --channel stable

# 更新到 Beta 版（尝鲜）
openclaw update --channel beta

# 更新到开发版（最新功能，可能不稳定）
openclaw update --channel dev
```

三个更新渠道的区别：

渠道	更新频率	稳定性	适合人群
stable	每周数次	高	大多数用户
beta	几乎每天	中	想尝鲜新功能的用户
dev	持续	低	开发者、贡献者

## 诊断检查 Diagnostics

安装完成后，运行诊断命令检查环境是否正常：

```
openclaw doctor
```

这个命令会检查：

- Node.js 版本是否满足要求 ( $\geq 22$ )
- 必要的系统依赖是否已安装
- Gateway 连接是否正常
- 已配置的模型 API Key 是否有效
- 守护进程状态
- 网络连通性

如果有任何问题，`openclaw doctor` 会给出具体的修复建议。这是排查问题的第一步。

## 本地备份 Backup (v2026.3.8+)

v2026.3.8 新增了本地备份工具，在执行破坏性操作前可以快速创建和验证备份：

```
# 创建完整备份
openclaw backup create

# 仅备份配置文件
openclaw backup create --only-config

# 验证备份完整性
openclaw backup verify
```

### 核心建议

养成定期备份的习惯。特别是在升级版本或修改配置前，先跑一次 `openclaw backup create`，出问题可以快速回滚。

**推荐版本：**截至 2026 年 3 月 11 日，推荐使用 v2026.3.8 稳定版。该版本在 v2026.3.7 的基础上增加了 ACP 身份验证、本地备份工具和 12+ 安全补丁。

## 15 渠道概览

### Channel Overview

OpenClaw 通过 Gateway 架构统一连接 20+ 聊天平台。所有渠道共享同一套三步接入模式：创建凭证 → 写入配置 → 启动 Gateway。

### 统一接入流程



可以同时运行多个 channel，消息自动路由到对应平台。配对模式 (`dmPolicy: pairing`) 默认启用，未知发送者需要验证码才能与 bot 对话。

## 完整平台列表

渠道	SDK / 实现	类型	难度	耗时
Telegram	grammY	内置	极简	5 分钟
Discord	discord.js	内置	简单	15-20 分钟
WhatsApp	Baileys	内置	中等	10-15 分钟
Slack	Bolt	内置	中等	25-40 分钟
Signal	Signal-CLI	内置	中等	20-30 分钟
iMessage	BlueBubbles	扩展	中等偏难	30-45 分钟
Google Chat	官方 API	内置	中等	15-20 分钟
LINE	官方 API	扩展	中等	15-20 分钟
Microsoft Teams	官方 API	扩展	中等	20-30 分钟
Matrix	协议实现	扩展	中等	15-20 分钟
Mattermost	官方 API	扩展	中等	15-20 分钟
IRC	协议实现	扩展	中等	10-15 分钟
Nostr	协议实现	扩展	中等	15-20 分钟
Twitch	官方 API	扩展	中等	15-20 分钟
Synology Chat	官方 API	扩展	中等	15-20 分钟
BlueBubbles	API	扩展	中等偏难	30-45 分钟
Zalo	API	扩展	中等	15-20 分钟
Nextcloud Talk	API	扩展	中等	15-20 分钟
Tlon	协议实现	扩展	中等	15-20 分钟
QQ	官方插件	插件	简单	5 分钟
飞书	官方 API	内置插件	中等	15-20 分钟

渠道	SDK / 实现	类型	难度	耗时
钉钉	社区插件	插件	中等	20-30 分钟
企业微信	社区插件	插件	中等	20-30 分钟
微信 (个人)	社区 / 第三方	插件	复杂	1 小时+
浏览器 (Chrome)	Browser Relay 扩展	内置 (v3.13新增)	简单	5-10 分钟

## 新手推荐排序

**从易到难推荐：**Telegram（最简单，5分钟零门槛）→ QQ（国内首选，扫码即用）→ 浏览器Chrome（5分钟，直接接管已登录账号）→ Discord（社区场景佳）→ 飞书（国内企业）→ 钉钉（社区插件成熟）→ WhatsApp（海外日常通讯）

梯队	平台	推荐理由
第一梯队 5-10 分钟	Telegram、QQ	Telegram 不需公网 IP、不需反向代理，本地 long-polling 即可运行。QQ 有腾讯官方支持，扫码 1 分钟绑定。
第二梯队 15-20 分钟	Discord、飞书	Discord 文档齐全，权限设置步骤略多但清晰。飞书自 OpenClaw 2026.2 起内置支持，适合国内企业。
第三梯队 25-40 分钟	WhatsApp、Slack、钉钉、企业微信	WhatsApp 最受欢迎但 session 可能过期。Slack 权限配置较多。钉钉和企业微信社区插件成熟。
第四梯队 需额外条件	iMessage、微信个人号	iMessage 需要 Mac 常开运行 BlueBubbles。微信个人号没有官方 API，封号风险始终存在。

## 16 国际平台接入

### International Platforms

本章覆盖六大国际平台的详细接入步骤。每个平台从创建凭证到完成对话的全流程。

#### Telegram 推荐入门 · 5 分钟 · 零门槛

Telegram 是 OpenClaw 官方推荐的入门渠道。使用 long-polling 模式，bot 主动轮询 Telegram 服务器拉取消息，不需要公网 IP、反向代理或端口转发。本地开发、NAT 后面、防火墙内都能正常工作。

##### 1 找到 @BotFather

在 Telegram 搜索 @BotFather，这是 Telegram 官方的 Bot 管理工具。向它发送 /newbot 命令。

##### 2 创建 Bot

按提示设置 bot 的显示名称和 username（必须以 bot 结尾，如 my\_openclaw\_bot）。创建成功后，BotFather 会返回一个 Bot Token。

##### 3 配置到 OpenClaw

将 Token 写入 openclaw.yaml：

```
channels:
  telegram:
    enabled: true
    botToken: "YOUR_BOT_TOKEN"
    dmPolicy: pairing # 需配对码才能使用
```

##### 4 启动并配对

重启 Gateway。在 Telegram 中给你的 bot 发送任意消息，Gateway 会返回配对码，输入后即可开始对话。

#### 核心建议

Telegram 的 Bot API 9.5（2026年3月）新增了 sendMessageDraft 功能。国内用户需要代理访问 Telegram，但 bot 运行本身不受影响——只要运行 Gateway 的机器能访问 api.telegram.org 即可。

## Discord 社区场景首选 · 15-20 分钟

Discord 适合社区管理和团队协作场景。需要在 Developer Portal 创建 Application 和 Bot，权限设置步骤稍多但文档齐全。

### 1 创建 Application

前往 `discord.com/developers/applications`，点击 New Application，填写应用名称。

### 2 获取 Bot Token

进入 Bot 页面，点击 Reset Token，复制生成的 Token。

### 3 启用 Privileged Intents

在 Bot 页面开启两个权限：**Message Content Intent** 和 **Server Members Intent**。没有这两个权限 bot 无法读取消息内容。

### 4 邀请 Bot 到服务器

在 OAuth2 → URL Generator 中勾选 `bot` scope 和所需权限，生成邀请链接，将 bot 添加到你的 Discord 服务器。

### 5 获取 ID 并配置

在 Discord 中开启 Developer Mode（设置 → 高级 → 开发者模式），右键复制 Server ID 和你的 User ID。将这些信息写入 `opencLaw.yaml`，启动 Gateway。

### 6 DM 配对

在 Discord 中私聊你的 bot，输入配对码（1 小时有效）完成绑定。

#### 核心建议

v2026.3.7 新增了 ACP 持久化频道绑定——Discord 频道和 Telegram 话题的绑定在 Gateway 重启后依然保持，不需要重新配对。

## WhatsApp 日常通讯 · 10-15 分钟

WhatsApp 是 OpenClaw 社区中最受欢迎的渠道。使用 Baileys 库通过 QR 码扫码连接，不需要 WhatsApp Business API。

### 1 运行交互式向导

安装 OpenClaw 后运行 `opencLaw onboard`，选择 WhatsApp 渠道。

## 2 扫码配对

终端会显示 QR 码。打开手机 WhatsApp → 设置 → 已连接设备 → 连接新设备，扫描 QR 码。

## 3 开始使用

配对完成后即可在 WhatsApp 中与 bot 对话。

### 注意

建议使用独立号码运行 WhatsApp，不要用主号。Gateway 运行时建议用 Node 而非 Bun（Bun 在 WhatsApp 场景下不稳定）。Session 凭证要当密码管理，session 过期需要重新扫码。

## Slack 企业/团队场景 · 25-40 分钟

Slack 适合企业和团队内部使用。需要在 Slack API 平台创建 App 并配置多项权限。默认使用 Socket Mode (WebSocket)，不需要公网 URL。

### 1 创建 Slack App

前往 `api.slack.com/apps`，点击 Create New App → From scratch，选择目标 Workspace。

### 2 启用 Socket Mode

在 Socket Mode 页面启用，生成 App-Level Token（以 `xapp-` 开头），scope 选择 `connections:write`。

### 3 配置 Bot Token Scopes

在 OAuth & Permissions 中添加权限：`chat:write`、`channels:history`、`channels:read`、`im:write`、`im:history`、`im:read`、`users:read`、`reactions:read`、`reactions:write`、`files:write`。

### 4 安装并配置

将 App 安装到 Workspace，获取 Bot User OAuth Token（以 `xoxb-` 开头）。将 Token 写入 `openclaw.yaml`，启动 Gateway。

### 注意

OpenClaw 可以在你的机器上执行真实命令，存在 prompt injection 风险。在 Slack 等多人环境中，建议不要在主力机器上运行 Gateway，使用 VM 或专用服务器。

## Signal 端到端加密 · 20-30 分钟

Signal 提供端到端加密通讯。OpenClaw 通过 Signal-CLI 工具连接 Signal 网络。

### 1 安装 Signal-CLI

根据操作系统安装 Signal-CLI。macOS 可通过 `brew install signal-cli`，Linux 从 GitHub Releases 下载。

### 2 注册或关联号码

使用 `signal-cli register` 注册新号码，或用 `signal-cli link` 关联已有 Signal 账号。

### 3 配置 OpenClaw

在 `openclaw.yaml` 中配置 Signal channel，指定号码和 Signal-CLI 路径，启动 Gateway。

## iMessage Apple 生态 · 30-45 分钟 · 需要 Mac

iMessage 接入通过 BlueBubbles 桥接实现（替代已废弃的 `imsg` channel）。需要一台常开的 Mac 作为 BlueBubbles Server。

### 1 安装 BlueBubbles Server

在 Mac 上从 `bluebubbles.app/install` 下载安装 BlueBubbles Server。推荐 macOS Sequoia (15) 或更新版本。

### 2 启用 Web API

在 BlueBubbles Server 设置中启用 Web API，设置访问密码。

### 3 配置 OpenClaw

在 `openclaw.yaml` 中配置 BlueBubbles channel：server URL、password、webhook 路径。

```
extensions:
  bluebubbles:
    enabled: true
    serverUrl: "http://localhost:1234"
    password: "YOUR_PASSWORD"
```

### 4 配置 Webhook

在 BlueBubbles 中添加 webhook 指向 Gateway：`https://gateway-host:3000/bluebubbles-webhook?password=<password>`。webhook 必须设置密码认证。

#### 注意

iMessage 通过 BlueBubbles 支持编辑、撤回、特效和表情回应。但 macOS 26 Tahoe 上编辑功能存在回归 bug（issue #32275）。Mac 必须保持开机运行 BlueBubbles Server。

## 17 国内平台接入

### Chinese Platforms

国内 IM 生态的 OpenClaw 支持正在快速发展。QQ 和飞书已有官方级支持，钉钉和企业微信社区插件成熟，微信个人号仍是技术挑战。

#### QQ 国内首选 · 扫码即用

QQ 是国内用户接入 OpenClaw 最简单的方式。腾讯官方开放了 QQ Bot 能力给 OpenClaw，扫码 1 分钟即可完成绑定。支持 Markdown、图片、语音、文件等多媒体消息，手机 QQ 和桌面 QQ 均可使用。

##### 1 注册 QQ Bot 开发者

用手机 QQ 扫码完成开发者注册。未实名认证的账号需要先完成实名。单个账号最多创建 5 个 Bot。

##### 2 创建 QQ Bot

在 QQ 开放平台一键创建 Bot，获取 App ID 和 Token。

##### 3 配置 OpenClaw

在 OpenClaw 运行环境中完成配置绑定，即可在 QQ 上与 bot 对话。

#### 核心建议

QQ Bot 适合两种场景：个人助手（私聊模式）和 QQ 社群管理（群聊自动回复、批量处理、定时通知）。

#### 飞书 国内企业首选 · OpenClaw 2026.2 起内置

飞书自 OpenClaw 2026.2 起获得原生内置支持。使用 WebSocket 事件订阅，支持私聊、群聊、照片/文件/视频等多媒体消息。

##### 1 创建飞书应用

在飞书开放平台（[open.feishu.cn](https://open.feishu.cn)）创建企业自建应用，获取 App ID 和 App Secret。

##### 2 运行向导配置

运行 `openclaw onboard`，选择 Feishu channel，粘贴 App ID 和 App Secret。

##### 3 重启 Gateway

重启 Gateway 后即可在飞书中与 bot 对话。

**社区替代方案：** 如果不想用内置插件，AlexAnys/feishu-openclaw 提供独立 bridge，不需要公网服务器、域名或 ngrok，5 分钟即可部署。AlexAnys/openclaw-feishu 仓库有保姆级配置指南，含 API 耗尽排查和 Lark Webhook 内网穿透方案。

## 钉钉 社区插件 · Stream 模式免公网

钉钉通过社区插件接入 OpenClaw。消息接收使用 Stream 模式（WebSocket 长连接），不需要公网地址。支持私聊、群聊、文件附件、语音消息、钉钉文档 API、多 Agent 路由等功能。

### 1 创建钉钉应用

在钉钉开放平台创建应用，添加机器人能力。

### 2 设置 Stream 模式

将消息接收模式设置为 Stream 模式。这样 bot 通过 WebSocket 长连接接收消息，不需要配置公网回调地址。

### 3 安装插件并配置

安装社区插件 `@soimy/dingtalk`，或使用 DingTalk-Real-AI 官方出品的 `dingtalk-openclaw-connector`（支持 AI Card 流式响应）。配置 `openclaw.yaml` 后启动 Gateway。

#### 核心建议

钉钉尚未获得 OpenClaw 官方内置支持（2026年3月有 Feature Request 提出），但社区方案已经非常成熟。DingTalk-Real-AI 连接器由钉钉团队维护，可靠性有保障。

## 企业微信 两种模式 · 已被多家云平台验证

企业微信有两种接入模式：Agent 模式（XML 回调经典模式）和 Bot 模式（JSON 回调，原生 stream 支持）。已被腾讯云、火山引擎、天翼云等公有云平台采纳验证。

### 1 创建企业微信应用

在企业微信管理后台创建自建应用（Agent 模式）或配置智能机器人（Bot 模式）。

### 2 安装社区插件

可选插件：`dingxiang-me/OpenClaw-Wechat`（支持个人微信互通、流式输出、群聊@、白名单控制、全中文配置）或 `sunnyy/openclaw-plugin-wecom`（支持动态 Agent 管理、指令白名单）。

### 3 配置并启动

按插件文档配置 `openclaw.yaml`，启动 Gateway。要求 OpenClaw  $\geq$  2026.2.9，部分功能需  $\geq$  2026.3.2。

#### 微信个人号 需求最大但最复杂

个人微信没有官方 Bot API，所有方案都是非官方的，封号风险始终存在。以下三种方案各有局限。

##### 方案 A：企业微信中转（推荐）

通过企业微信接入 OpenClaw，再用微信插件打通企业微信和个人微信。合法合规，在微信生态内，需要企业微信管理后台权限。

##### 方案 B：iPad 协议 + 中转网关

不走 Web 协议（高风险封号），走 iPad 协议。稳定性更高但技术门槛也更高。社区项目：

`freestylefly/openclaw-wechat`、`laolin5564/openclaw-wechat`。

##### 方案 C：微信小程序

2026 年新方案，通过小程序对接 OpenClaw。阿里云/腾讯云有预置镜像，降低部署门槛。

#### 注意

个人微信的所有接入方案都需要持续维护——协议更新可能导致不可用，iPad 协议相对安全但不是零风险。建议不要用常用的主号，使用备用号测试。云端部署才能保证 24 小时在线。

#### openclaw-china 统一插件 一站式国内平台支持

BytePioneer-AI/openclaw-china 提供一站式国内平台支持，覆盖飞书、钉钉、QQ、企业微信、微信五个平台。

```
git clone https://github.com/BytePioneer-AI/openclaw-china.git
cd openclaw-china
pnpm install && pnpm build
openclaw china setup # 交互式配置向导
```

特色功能包括：交互式配置向导减少手动配置、企业微信 MP4 视频播放器和多文件类型发送、腾讯云 ASR 语音转文字、钉钉日志增强（userId/groupId 定位问题）。

**选择建议：**如果只用一个国内平台，直接安装对应的独立插件更轻量。如果要同时接入多个国内平台，openclaw-china 统一包更省事。

## 18 远程访问

### Remote Access

OpenClaw Gateway 默认监听本地 `ws://127.0.0.1:18789`。当你需要从外部网络访问时，有以下几种方案。

### Tailscale Serve / Funnel 推荐方案

Tailscale 是 OpenClaw 官方推荐的远程访问方案，提供两种模式：

模式	访问范围	使用场景
Serve	Tailscale 网络内的设备	自己的手机/平板访问家里的 OpenClaw
Funnel	公网任何人	给 webhook 回调提供公网 URL（如飞书、Slack HTTP 模式）

```
# Serve: 仅 Tailscale 网络可访问
tailscale serve --bg https+insecure://127.0.0.1:18789

# Funnel: 公网可访问 (用于 webhook 回调)
tailscale funnel --bg https+insecure://127.0.0.1:18789
```

#### 核心建议

大部分 channel（Telegram long-polling、Discord、Slack Socket Mode、钉钉 Stream 模式）都是 bot 主动连接服务器，不需要公网 IP。只有需要 webhook 回调的场景（BlueBubbles、Slack HTTP 模式）才需要 Funnel 暴露公网地址。

### SSH 端口转发 最通用的方案

如果 OpenClaw 运行在远程服务器上，用 SSH 隧道将 Gateway 端口转发到本地：

```
# 将远程服务器的 18789 端口转发到本地
ssh -L 18789:127.0.0.1:18789 user@your-server

# 后台运行
ssh -fNL 18789:127.0.0.1:18789 user@your-server
```

转发后，本地客户端连接 `ws://127.0.0.1:18789` 即可访问远程 Gateway。

## Dashboard Web UI (v2026.3.12 全面升级)

v2026.3.12 推出了 Dashboard v2，控制台从功能型界面升级为完整的模块化管理中心：

视图	功能
Overview	Agent 状态总览、Token 用量、渠道连接状况
Chat	斜杠命令、消息搜索、导出、置顶消息
Config	模型配置、渠道开关、Plugin 管理
Agent	记忆查看、Cron 任务管理
Session	多会话管理、历史记录

```
# Gateway 启动后默认可访问
# 浏览器打开 http://127.0.0.1:18789
openclaw gateway --port 18789 --verbose
```

新增命令面板 (Command Palette)，按 **⌘K** 快速跳转。移动端新增底部标签栏，代替原来的悬浮按钮。

**安全提醒：** v2026.3.7 起 Gateway 认证要求显式设置 `gateway.auth.mode` (token 或 password)。v2026.3.12 设备配对改用 Ephemeral Token，连接更安全。不要在公网暴露未认证的 Gateway。

## Chrome 浏览器接入 v2026.3.13 新增 · 5-10 分钟

v2026.3.13 新增了最特别的一种「渠道」：直接附着到你正在使用的 Chrome 浏览器。Agent 可以操控你已经登录的账号和页面——不需要另起账号，不需要 API Key，直接接管你的浏览器会话。

相比之前的浏览器工具 (无头模式)，这个方案的核心优势是：**利用现有登录状态**。Agent 不需要再去登录各种网站，直接用你已经登录的状态操作。

### 1 安装 Browser Relay 扩展

在 Chrome 网上应用店安装 **OpenClaw Browser Relay** 扩展 (扩展 ID:

`nglingapjinhecnfejdcpihlpneeadjp`)。

## 2 启动带调试端口的 Chrome

关闭所有 Chrome 窗口后，通过以下方式重新启动：

```
# macOS
open -a "Google Chrome" --args --remote-debugging-port=9222

# Windows
"C:\Program Files\Google\Chrome\Application\chrome.exe" --remote-debugging-port=9222
```

或者在 `openclaw.yaml` 中使用内置 Profile 快捷方式：

```
browser:
  profile: "user" # 使用用户默认 Profile
  # profile: "chrome-relay" # 使用中继模式
```

## 3 在 OpenClaw 中启用浏览器渠道

在 `openclaw.yaml` 中启用浏览器工具：

```
tools:
  browser:
    enabled: true
    attachMode: "devtools" # v3.13 新增，附着到已有会话
```

## 4 向 Agent 下达浏览器任务

重启 Gateway 后，直接给 Agent 发送浏览器相关指令，例如：「帮我整理浏览器里所有打开的 GitHub PR」「把这个表单填写完」「截图保存当前页面」。

### 核心建议

v2026.3.13 还支持 browser act batching：把多个浏览器操作打包成批次执行，减少来回通信，自动化操作更稳定，不容易因为页面渲染时机问题卡住。

### 注意

Chrome DevTools 附着模式意味着 Agent 可以读取你浏览器中所有页面的内容，包括已登录账号的私人信息。仅在信任的 Agent 配置下使用，不要在公共电脑或不受控的服务器上启用此功能。

## macOS 菜单栏伴侣应用

OpenClaw 提供 macOS 原生客户端（`apps/macos/`），以菜单栏常驻应用的形式运行。功能包括：

- 一键启动/停止 Gateway

- 查看当前连接的 channel 状态
- 快速访问 Dashboard Web UI
- 系统通知（新消息、配对请求等）

iOS 和 Android 客户端也在开发中（`apps/ios/`、`apps/android/`），代码已在主仓库中。

#### 核心建议

如果你同时使用多台设备，推荐 Tailscale Serve + macOS 菜单栏应用的组合：Mac 运行 Gateway 和菜单栏应用，手机/平板通过 Tailscale 网络访问。

## 19 Skills工作原理

### How Skills Work

Skills是OpenClaw的能力扩展单元。理解它的加载机制，才能真正用好这个系统。

### 三层优先级

OpenClaw的Skill有三个来源，按优先级从高到低排列：

优先级	位置	说明
最高	<code>&lt;workspace&gt;/skills/</code>	项目级Skills，只对当前工作区生效。适合针对特定项目定制的能力。
中	<code>~/.openclaw/skills/</code>	用户级Skills，全局生效。通过ClawHub安装或手动放置的Skills都在这里。
最低	bundled skills	内置的55个Skills，随OpenClaw版本发布。不需要安装，开箱即用。

#### 核心建议

如果同名Skill存在于多个层级，高优先级会覆盖低优先级。这意味着你可以在workspace级别「重写」一个内置Skill的行为，而不影响其他项目。

### Skill加载过程

当OpenClaw启动或收到消息时，Skills的加载遵循以下流程：

#### 1 读取Skill元数据

扫描三层目录，读取每个Skill的 `SKILL.md` 文件，解析名称、描述、触发条件、所需环境变量等元信息。

#### 2 应用环境变量

如果Skill声明了需要的API Key或环境变量（如 `GITHUB_TOKEN`），系统会从 `openclaw.json` 的 `env` 字段中注入。缺少必要变量的Skill会被静默跳过。

#### 3 构建System Prompt

将所有可用Skills的描述注入到system prompt中，告知模型当前可以调用哪些能力。这是模型「知道自己能做什么」的关键步骤。

#### 4 运行后恢复

Skill执行完毕后，恢复原始环境变量和上下文状态，避免Skill之间互相干扰。

### ClawHub注册表

ClawHub ([clawhub.com](http://clawhub.com)) 是OpenClaw的官方Skill注册表，类似npm之于Node.js。它提供：

- 公共Skills的发布和版本管理
- 基于向量搜索的Skill发现
- 下载量统计和社区评分
- VirusTotal合作的安全扫描（但覆盖率有限）

## 20 ClawHub与技能生态

### ClawHub & Skill Ecosystem

13,729个技能只是冰山一角。加上Skills.sh的8.7万和SkillsMP的40万+, Agent技能生态正在爆发。

### 市场概况

指标	数据
总注册技能	13,729
精选技能 (awesome列表筛选)	5,494
被过滤技能 (垃圾/重复/恶意)	6,940
被标记为恶意的	800+ (约20%在高峰期)

#### 注意

ClawHub的质量问题非常严重。社区项目 awesome-openclaw-skills (31.4K Stars) 从13,729个技能中只精选了5,494个, 剩下的大部分是垃圾、重复或低质量内容。安装任何第三方Skill前, 务必查看源码。

### 安装与搜索

```
# 安装Skill
openclaw skills install <skill-name>

# 搜索Skill
openclaw skills search "browser automation"

# 列出已安装的Skills
openclaw skills list

# 卸载Skill
openclaw skills uninstall <skill-name>
```

ClawHub支持向量搜索, 也就是说你可以用自然语言描述需求来搜索Skill, 不必精确匹配名称。

## 技能分类Top 10

排名	分类	数量	说明
1	编码Agent与IDE	1,222	代码生成、调试、重构等开发辅助
2	Web与前端开发	938	HTML/CSS/JS生成、组件开发
3	DevOps与云	408	Docker、K8s、CI/CD管理
4	搜索与研究	350	联网搜索、信息汇总
5	浏览器与自动化	335	网页操作、表单填写、截图
6	生产力与任务	206	日程、待办、项目管理
7	AI与LLM	197	提示工程、模型切换、多Agent协作
8	CLI工具	186	终端命令增强、系统管理
9	Git与GitHub	170	仓库管理、PR审查、Issue处理
10	图片与视频生成	169	AI绘图、视频处理

编码相关的技能占了绝大多数（前两名合计2,160个），反映出OpenClaw用户中开发者占比极高。但也意味着这两个分类里重复和低质量Skill最多。

## 第三方技能平台

ClawHub不是唯一的选择。2026年初，多个第三方技能平台相继上线，形成了一个跨Agent的技能共享生态。

平台	技能数量	出品方	定位	支持的Agent
ClawHub	13,729	OpenClaw 官方	策展市场（App Store式），有向量搜索和版本回滚	仅OpenClaw
Skills.sh	87,918	Vercel	开放市场（npm式），体量最大，跨Agent兼容	Claude Code、Cursor、Copilot、Codex、OpenClaw等20+
SkillsMP	400,000+	社区	社区爬取GitHub的SKILL.md文件，数量最多但质量参差	通用
SkillHub	7,000+	社区	每个Skill有AI自动评分，质量控制更好	通用
扣子 Skills	早期阶段	字节跳动	技能商店+付费变现，支持「一句话生成」技能	扣子Agent

## Skills.sh: Agent技能的npm

Vercel在2026年1月20日推出的Skills.sh是目前体量最大的跨平台技能市场。它的核心理念是：一个Skill应该能在任何Agent中运行，不绑定特定平台。

```
# 从Skills.sh安装技能（一行命令）
npx skills add owner/repo-name
```

Skills本质上是结构化指令文件（SKILL.md），注入Agent的上下文窗口，提供特定领域的程序化知识。它坐在MCP之上：MCP解决「Agent怎么连工具」，Skills解决「Agent怎么用好工具」。

## MCP生态与Skills的融合

MCP（Model Context Protocol）已捐赠给Linux基金会，成为Agent工具连接的事实标准。截至2026年3月：

- mcp.so收录18,420+ MCP Servers
- Smithery托管3,300-7,300+ MCP Server
- 已出现skill-to-mcp桥接工具，两套生态正在融合

一个趋势正在形成：MCP负责「连接」（让Agent能调用外部工具），Skills负责「智慧」（教Agent如何高效使用工具）。两者互补而非竞争。

**实用建议：**如果你已经在用Claude Code或Cursor等编程工具，可以从Skills.sh安装技能来增强能力，这些技能和OpenClaw的ClawHub Skills使用相同的SKILL.md格式。跨平台复用是未来的大趋势。

## 21 热门Skills推荐

### Top Skills

55个内置技能开箱即用，加上社区精选的必装Top 10。

### 必装Top 10

排名	Skill名称	下载量	用途
1	Gmail / Google	32K+	邮件收发、日历管理、Google Docs读写。基础设施级Skill，几乎所有用户都在用。
2	Agent Browser	高	浏览器自动化：登录后台、填写表单、截图、导出PDF。基于Chrome DevTools Protocol。
3	Summarize	高	视频、网页、邮件内容的自动摘要。日常使用频率最高的Skill之一。
4	GitHub	高	仓库管理、Issue处理、PR审查。技术用户标配，大幅减少网页操作时间。
5	Claude Code	中	通过MCP协议桥接Claude Code能力（Bash、Read、Write、Edit等），让OpenClaw获得专业编程能力。
6	Web Search	高	联网搜索，让Agent能获取实时信息。支持多个搜索引擎后端。
7	File Manager	中	本地文件的读写、移动、重命名等操作。需要注意安全权限。
8	Calendar	中	日程查看与管理，支持Google Calendar等多个日历服务。
9	Translator	中	多语言翻译。对跨语言交流场景非常实用。
10	Image Gen	中	AI图片生成，集成DALL-E、Stable Diffusion等后端。

### 内置55个技能分类一览

#### 通讯与社交

discord slack imsg (iMessage) bluebubbles wacli (WhatsApp CLI) voice-call

#### 笔记与知识管理

obsidian notion apple-notes bear-notes trello things-mac apple-reminders

## 开发工具

coding-agent github gh-issues tmux

## 媒体处理

spotify-player songsee sonoscli video-frames openai-image-gen gifgrep camsnap

## AI与模型

gemini openai-whisper openai-whisper-api sherpa-onnx-tts model-usage

## 搜索与浏览

xurl summarize blogwatcher gog (Google搜索) goplaces

## 系统工具

1password healthcheck session-logs himalaya (邮件CLI) peekaboo oracle canvas

## 智能家居

openhue (Philips Hue灯光控制)

## 生态工具

clawhub (技能商店客户端) skill-creator (技能创建器) mcporter (MCP桥接)

**实用建议：**不要一次性安装太多Skills。每个Skill都会增加system prompt的长度，占用上下文窗口。建议从Top 10中选择你真正需要的3-5个开始，用熟了再逐步扩展。

## 22 自建Skill指南

### Create Your Own Skill

一个Skill的最小单位就是一个目录加一个 SKILL.md 文件。

### 目录结构

```
my-skill/ |—— SKILL.md # 必须。Skill的核心定义文件 |—— scripts/ # 可选。辅助脚本 |——  
helper.py |—— templates/ # 可选。模板文件 |—— report.md |—— README.md # 可选。说明文档
```

唯一必须的文件是 `SKILL.md`，其他都是可选的。最简单的Skill只需要一个SKILL.md就能工作。

### SKILL.md格式示例

```
# My Custom Skill  
  
## Description  
帮助用户进行每日工作总结，生成结构化的日报。  
  
## Trigger  
当用户提到「日报」「工作总结」「今日汇报」时激活。  
  
## Instructions  
1. 询问用户今天完成了哪些工作  
2. 按项目分类整理  
3. 标注每项工作的状态（已完成/进行中/阻塞）  
4. 生成markdown格式的日报  
5. 保存到 ~/reports/YYYY-MM-DD.md  
  
## Environment Variables  
- REPORTS_DIR: 日报存储目录（默认 ~/reports）  
  
## Tools Required  
- file_write  
- memory_search
```

## 安装方式

方式	位置	生效范围	命令
项目级	<code>&lt;workspace&gt;/skills/my-skill/</code>	仅当前工作区	直接将文件夹放到workspace的skills目录下
全局	<code>~/.openclaw/skills/my-skill/</code>	所有会话	直接复制，或通过ClawHub安装

### 核心建议

项目级Skill非常适合团队协作场景：把Skill放进Git仓库的 `skills/` 目录，团队成员克隆仓库后就自动获得了相同的Agent能力。

## 分享到ClawHub

### 1 准备Skill

确保SKILL.md格式正确，包含清晰的Description和Instructions。

### 2 登录ClawHub

```
openclaw clawhub login
```

### 3 发布

```
openclaw clawhub publish ./my-skill
```

发布后其他用户可以通过 `openclaw skills install your-skill-name` 安装。ClawHub会自动进行基础安全扫描，但不保证完全可靠（见下一节）。

## 23 Skills安全

### Skill Security

ClawHavoc供应链攻击是OpenClaw历史上最严重的安全事件之一。每个「养虾人」都应该了解。

### ClawHavoc供应链攻击

2026年1月底到2月初，OpenClaw社区遭遇了一场大规模供应链攻击，被安全研究机构Koi Security命名为「ClawHavoc」。

#### 时间线

日期	事件
1月27日	首个恶意Skill出现在ClawHub上，伪装成专业工具
1月28-30日	攻击者快速上传大量恶意Skill，利用ClawHub缺乏审查机制的漏洞
1月31日	攻击全面爆发，多名用户报告异常行为
2月1日	Koi Security正式命名该攻击为「ClawHavoc」
2月上旬	社区展开大规模审计和清理

#### 攻击规模

指标	数据
当时ClawHub技能总数	约2,857个
初步确认恶意Skills	341个 (约12%)
后续扫描发现的恶意Skills	800+ (约20%)
可追溯到同一协调行动的	335个
受影响设备	135,000+

#### 注意

ClawHub当时约20%的Skills被确认为恶意。这意味着如果你随机安装5个Skill，大概率至少有1个是恶意的。

## 攻击手法

攻击者的手法相当精密：

- 上传看似专业的Skill，名称和描述都很正常（如「advanced-code-review」「smart-scheduler」）
- 诱导用户安装后，Skill会建议安装一个「helper agent」来增强功能
- 实际植入的是 Atomic macOS Stealer（AMOS）信息窃取木马
- 更危险的是：攻击专门针对OpenClaw的持久记忆文件（SOUL.md 和 MEMORY.md），篡改Agent的长期行为指令

篡改SOUL.md意味着你的Agent被「洗脑」了。它的核心行为准则被改写，可能在后续所有交互中执行恶意操作，而你完全不知情。

## 安全建议

### 1 安装前审查源码

永远不要盲目安装ClawHub上的Skill。去GitHub查看源码，确认SKILL.md中没有可疑的指令。特别注意任何要求额外安装「helper」或「agent」的内容。

### 2 使用SecureClaw扫描

社区推出了开源安全工具SecureClaw，可以扫描已安装的Skills检查恶意内容。虽然不能100%防护，但能拦住已知的攻击模式。

```
# 安装SecureClaw
npm install -g secureclaw

# 扫描已安装的skills
secureclaw scan ~/.openclaw/skills/
```

### 3 优先使用精选列表

参考 awesome-openclaw-skills 项目（31.4K Stars）的精选列表，而不是直接在ClawHub上随意搜索。精选列表已经过滤掉了大量垃圾和恶意Skill。

### 4 定期检查SOUL.md和MEMORY.md

养成习惯，定期检查这两个文件有没有被异常修改。如果发现不认识的内容，立即回滚并排查所有已安装的Skill。

## 2026年3月：VirusTotal审计发现100+恶意Skills

VirusTotal 对 ClawHub 进行了安全审计，发现超过 100 个 Skills 包含恶意代码，类型包括加密货币窃取、反向 Shell 后门和凭证窃取。这些恶意 Skill 并非来自 ClawHavoc 时期的残留，而是持续新增的。这说明 ClawHub

的安全审核机制仍然不够完善，安装第三方 Skill 的风险并未随着时间降低。

#### 注意

安全红线：拒绝任何要求你「下载 zip 文件」「执行 shell 脚本」「输入密码」的 Skill。这些是恶意 Skill 最常见的行为模式。

**关键认知：**OpenClaw的Skill本质上是受信任代码。一旦安装，它就拥有和你的OpenClaw实例相同的权限。没有沙箱隔离，没有权限分级。这和npm生态早期面临的问题一模一样，但后果可能更严重，因为OpenClaw可以访问你的邮件、日历、消息和文件系统。

---

## 24 模型提供商总览

### *Provider Overview*

OpenClaw支持十余家模型提供商，从国际顶尖到国产平价再到完全免费的本地模型，覆盖所有预算和场景。

OpenClaw最大的优势之一是模型自由：你不会被绑定在某一家厂商上。通过 `~/.openclaw/openclaw.json` 配置文件，可以灵活切换主力模型、设置Fallback备选链、甚至让不同任务走不同模型。

## 支持的模型提供商一览

提供商	代表模型	输入价格 /1M tokens	输出价格 /1M tokens	接入方式	推荐场景
Anthropic	Claude Sonnet 4.6	\$3.00	\$15.00	内置Provider	Agent任务效果最佳
OpenAI	GPT-5.4	\$2.50	\$15.00	内置Provider	通用能力强
Google	Gemini 3 Pro	\$2.00	\$12.00	内置Provider	多模态、超长上下文
DeepSeek	DeepSeek-V3.2.2 / V4	\$0.14	\$0.28	自定义 Provider	极致低价、代码任务
智谱GLM	GLM-5	\$0.80	\$2.56	内置 (zai)	国产最强代码能力
智谱GLM	GLM-5-Turbo	\$0.96	\$3.20	内置 (zai)	<b>NEW</b> 首个专为OpenClaw训练优化的模型
通义千问	Qwen 3.5 Max	\$1.20	\$6.00	插件 (OAuth)	中文NLP、代码生成
豆包	Seed 2.0 Pro	\$0.47	\$2.37	自定义 Provider	批量处理、低成本
百度文心	文心 5.0	~\$0.58	~\$1.16	自定义 (需适配)	百度云生态用户
Kimi	Kimi K2.5	\$0.60	\$3.00	自定义 Provider	中文Agent、长上下文
MiniMax	MiniMax M2.5	\$0.50	\$2.00	自定义 Provider	SWE-bench高分、性价比
Ollama	Qwen3.5-Coder:32B	免费	免费	自动发现	隐私敏感、零成本
LM Studio	Devstral-24B	免费	免费	自定义 Provider	本地GUI、模型测试

## 配置核心概念

理解三个关键概念，就能掌握OpenClaw的模型配置：

- **内置Provider**：Anthropic、OpenAI、Google、智谱 (zai) 等无需额外配置，设置API Key即可使用

- **自定义Provider**: DeepSeek、豆包、Kimi等需要在 `models.providers` 中手动添加
- **Fallback机制**: 主模型不可用时自动切换到备选，这是最核心的省钱策略

```
{
  env: { "API_KEY_NAME": "sk-xxx" },
  agents: {
    defaults: {
      model: {
        primary: "provider/model-name",    // 主力模型
        fallbacks: ["provider/model-b"]    // 备选（主模型限速时自动切换）
      }
    }
  },
  models: {
    mode: "merge", // 保留内置provider，叠加自定义
    providers: { /* 自定义provider配置 */ }
  }
}
```

#### 核心建议

设置 `models.mode: "merge"` 非常重要。它能保留所有内置Provider的同时叠加你的自定义配置。如果不设置，自定义配置会覆盖内置Provider。

## 25 国际模型配置

### International Models

Anthropic Claude、OpenAI GPT、Google Gemini的完整配置指南。

### Anthropic Claude

Claude是OpenClaw的默认模型提供商，也是社区公认的Agent任务效果最好的模型。Sonnet 4.6在工具调用的准确率和稳定性上显著领先其他模型。

模型	输入 /1M	输出 /1M	上下文	定位
Claude Opus 4.6	\$5.00	\$25.00	200K	最强推理，复杂任务
Claude Sonnet 4.6	\$3.00	\$15.00	200K	主力模型，性价比之选
Claude Haiku 4.5	\$1.00	\$5.00	200K	轻量任务，高速低成本

### 配置方式

Claude是内置Provider，配置最简单：

```
# 环境变量方式
ANTHROPIC_API_KEY=sk-ant-xxx

# 或在 openclaw.json 中设置
{
  env: { "ANTHROPIC_API_KEY": "sk-ant-xxx" }
}
```

模型ID： `anthropic/claude-opus-4-6`、`anthropic/claude-sonnet-4-6`、`anthropic/claude-haiku-4-5`

#### 注意

Anthropic已封杀OAuth认证方式。使用Claude Pro/Max订阅账户通过OAuth连接OpenClaw的用户会收到警告甚至被锁定账户。目前唯一合法路径是使用API Key（按量付费）。

### 省钱技巧：

- Batch API可享50%折扣（输入输出均半价）
- Prompt Caching可降低重复上下文成本达90%

- 日常任务用Sonnet即可，复杂任务再升级Opus

## OpenAI GPT

模型	输入 /1M	输出 /1M	上下文	定位
GPT-5.4	\$2.50	\$15.00	272K (标准)	最新旗舰
GPT-5.4 (>272K)	\$5.00	\$15.00	1.05M	超长上下文
GPT-5.2	\$1.75	\$14.00	—	上一代旗舰
GPT-5	\$1.25	\$10.00	—	性价比之选

### 配置方式

```
OPENAI_API_KEY=sk-xxx
```

#### 注意

GPT-5.4超过272K上下文后输入价格翻倍（\$2.50→\$5.00）。如果你的Agent会话上下文较长，注意控制长度或设置消费限额。

## Google Gemini

模型	输入 /1M	输出 /1M	上下文	定位
Gemini 3 Pro (≤200K)	\$2.00	\$12.00	200K	旗舰多模态
Gemini 3 Pro (>200K)	\$4.00	\$18.00	2M	超长上下文
Gemini 3 Flash	\$0.50	\$3.00	—	高速低成本

### 配置方式

```
GOOGLE_API_KEY=xxx  
# 或通过 Google AI Studio 免费额度使用
```

Gemini的独家优势是2M上下文窗口和慷慨的免费额度（Flash每日有免费请求）。多模态能力也是三家中最强的。

### 核心建议

Gemini Flash的免费额度非常适合用作心跳（Heartbeat）和定时任务（Cron）的模型，这些场景不需要最强能力但需要持续运行，用免费模型可以把成本降到零。

## 26 国产模型配置

### Chinese Models

国产模型是OpenClaw用户省钱的核心武器。DeepSeek-V3.2.2的输入价格仅为Claude Sonnet的1/20。

### DeepSeek

性价比之王。DeepSeek-V3.2.2是当前稳定版（2025年12月发布），输入价格仅\$0.14/M tokens，是目前OpenClaw社区最常用的低成本模型。

模型	输入 /1M	输出 /1M	定位
DeepSeek-V3.2.2 (deepseek-chat)	\$0.14	\$0.28	当前稳定版，极致低价
DeepSeek-R1 (deepseek-reasoner)	\$0.55~0.70	\$2.19~2.50	深度推理

### 配置方式（自定义Provider）

```
{
  env: { "DEEPSEEK_API_KEY": "sk-xxx" },
  models: {
    mode: "merge",
    providers: {
      deepseek: {
        baseUrl: "https://api.deepseek.com/v1",
        apiKey: "${DEEPSEEK_API_KEY}",
        api: "openai-completions",
        models: [
          { id: "deepseek-chat", contextWindow: 128000, maxTokens: 8192 },
          { id: "deepseek-reasoner", contextWindow: 128000, maxTokens: 8192 }
        ]
      }
    }
  }
}
```

#### 注意

DeepSeek高峰期偶有延迟甚至不可用，不建议作为唯一Provider。务必搭配Fallback模型兜底。

## 智谱GLM

国产模型中代码能力最强的选择。GLM-5在SWE-bench上拿到了开源模型最高分，价格仅\$0.80/M输入。更妙的是，OpenClaw内置了zai Provider，配置极为简单。

模型	输入 /1M	输出 /1M	定位
GLM-5-Turbo	\$0.96	\$3.20	🆕 首个专为 OpenClaw 优化的基座模型
GLM-5	\$0.80	\$2.56	旗舰，代码能力强
GLM-4.5	\$0.60	\$2.20	上一代主力
GLM-4.7-Flash	免费	免费	轻量免费
GLM-4.5-Flash	免费	免费	轻量免费

### 🆕 GLM-5-Turbo：第一个「龙虾模型」

2026年3月16日，智谱发布 GLM-5-Turbo，官方定位是「首个龙虾模型」——历史上第一个从训练阶段就专为 OpenClaw 使用场景深度优化的基座模型。和普通大模型接入 OpenClaw 不同，GLM-5-Turbo 在训练时就针对了四个 OpenClaw 核心能力：

- **工具调用 (Tool Calling)**：更准确的工具选择和参数传递
- **指令跟踪 (Command Following)**：多步骤任务不丢失上下文
- **持久任务 (Persistent Tasks)**：长时间运行不降级
- **长链执行 (Long-chain Execution)**：减少中途失败和幻觉

参数	GLM-5-Turbo
最大输出 Token	128K
上下文长度	200K
支持功能	思考模式 · 函数调用 · 流式输出 · 上下文缓存 · MCP
当前状态	已上线，闭源（已接入 OpenRouter / Coze / 美团 / Trae）
API 定价	输入 \$0.96/M · 输出 \$3.20/M（比 GLM-5 贵 20%）
龙虾套餐	体验月卡 ¥39（3500万 tokens）· 进阶月卡 ¥99（1亿 tokens）

## 配置方式

```

# GLM-5-Turbo (已上线, API直接可用)
{
  env: { "ZAI_API_KEY": "sk-xxx" },
  agents: {
    defaults: {
      model: { primary: "zai/glm-5-turbo" }
    }
  }
}

# GLM-5 (正式版, 推荐)
{
  env: { "ZAI_API_KEY": "sk-xxx" },
  agents: {
    defaults: {
      model: { primary: "zai/glm-5" }
    }
  }
}

```

CLI 快速配置: `openclaw onboard --auth-choice zai-api-key`。注意 `z.ai/*` 和 `z-ai/*` 前缀会自动转换为 `zai/*`。

#### 核心建议

GLM Flash 系列完全免费, 适合心跳任务和简单对话。GLM-5-Turbo 已上线并接入多个平台 (OpenRouter / Coze / 美团 / Trae), 「龙虾套餐」月卡 ¥39 起, 是国内 OpenClaw 用户的新选择。注意 GLM-5-Turbo 比 GLM-5 贵 20%, 如果你的 Agent 任务不重度依赖工具调用和长链执行, GLM-5 仍然是性价比更高的选择。

## 通义千问 Qwen

Qwen 3.5 是阿里 2026 年 2 月发布的最新版本 (397B 总参数/17B 激活, MoE 架构, 已开源)。代码专用的 Qwen3.5-Coder 性价比极高。

模型	输入 /1M	输出 /1M	定位
Qwen 3.5 Max	\$1.20	\$6.00	旗舰模型 (397B-A17B)
Qwen 3.5 Plus	\$0.40	\$1.20	主力平衡
Qwen 3.5 Coder	\$0.22	\$1.00	代码专用, 性价比极高
Qwen 3.5 8B	\$0.05	\$0.40	轻量低成本

### 配置方式 (插件 + OAuth)

```
# 通过插件接入, OAuth设备码认证 (无需API Key)
openclaw plugins enable qwen-portal-auth
openclaw gateway restart
openclaw models auth login --provider qwen-portal --set-default
```

模型ID: `qwen-portal/coder-model`、`qwen-portal/vision-model`。每日2,000次免费请求。

## 豆包 Doubao

模型	输入 /1M	输出 /1M	定位
Seed 2.0 Pro	\$0.47	\$2.37	旗舰推理, 对标GPT-5.2
Doubao 1.5 Pro-32k	\$0.11	—	通用对话, 极致低价
Doubao 1.5 Lite-32k	\$0.042	—	最便宜的选择之一

## 配置方式 (自定义Provider)

```
{
  env: { "DOUBAO_API_KEY": "xxx" },
  models: {
    mode: "merge",
    providers: {
      doubao: {
        baseUrl: "https://ark.cn-beijing.volces.com/api/v3",
        apiKey: "${DOUBAO_API_KEY}",
        api: "openai-completions",
        models: [
          { id: "doubao-seed-2.0-pro", contextWindow: 128000, maxTokens: 4096 }
        ]
      }
    }
  }
}
```

## Kimi (月之暗面)

模型	输入 /1M	输出 /1M	定位
Kimi K2.5	\$0.60	\$3.00	最新旗舰
Kimi K2 0905	\$0.39	\$1.90	性价比版

## 配置方式

```
{
  env: { "MOONSHOT_API_KEY": "sk-xxx" },
  models: {
    mode: "merge",
    providers: {
      moonshot: {
        baseUrl: "https://api.moonshot.cn/v1",
        apiKey: "${MOONSHOT_API_KEY}",
        api: "openai-completions",
        models: [
          { id: "kimi-k2.5", contextWindow: 256000, maxTokens: 8192 }
        ]
      }
    }
  }
}
```

也可通过OpenRouter接入：`openrouter/moonshotai/kimi-k2.5`

## 百度文心

文心5.0于2026年1月22日发布（2.4万亿参数，原生全模态，激活参数比<3%）。

模型	输入价格	输出价格	定位
文心 5.0	~\$0.58/M	~\$1.16/M	最新旗舰（2.4万亿参数）
ERNIE Speed	免费	免费	轻量
ERNIE Lite	免费	免费	最轻量

### 注意

百度API格式与OpenAI不完全兼容，需要通过one-api等中转工具适配。在OpenClaw社区中存在感最低，配置复杂度最高。如果没有特别的百度云生态绑定，建议优先选择其他国产模型。

## MiniMax

MiniMax M2.5（230B参数）在SWE-Bench上得分80.2%，代码能力突出。

模型	输入 /1M	输出 /1M	定位
MiniMax M2.5	\$0.50	\$2.00	旗舰，SWE-bench 80.2%

## 配置方式

```
{
  env: { "MINIMAX_API_KEY": "xxx" },
  models: {
    mode: "merge",
    providers: {
      minimax: {
        baseUrl: "https://api.minimax.chat/v1",
        apiKey: "${MINIMAX_API_KEY}",
        api: "openai-completions",
        models: [
          { id: "minimax-m2.5", contextWindow: 128000, maxTokens: 8192 }
        ]
      }
    }
  }
}
```

## 聚合平台：一个API Key调多个模型

### 硅基流动 SiliconFlow（国内首选）

国内最大的模型聚合平台，一个API调用多个开源模型，延迟低，有免费额度。

```
{
  env: { "SILICONFLOW_API_KEY": "sk-xxx" },
  models: {
    mode: "merge",
    providers: {
      siliconflow: {
        baseUrl: "https://api.siliconflow.cn/v1",
        apiKey: "${SILICONFLOW_API_KEY}",
        api: "openai-completions",
        models: [
          { id: "Pro/deepseek-ai/DeepSeek-V3.2", contextWindow: 128000, maxTokens: 8192 },
          { id: "Pro/zai-org/GLM-5", contextWindow: 128000, maxTokens: 8192 }
        ]
      }
    }
  }
}

// 设置默认模型
// openclaw config set agents.defaults.model.primary siliconflow/Pro/zai-org/GLM-5
```

### OpenRouter（国际首选）

290+模型，OpenClaw内置支持，但有5.5%平台费。

```
openclaw onboard --auth-choice apiKey --token-provider openrouter --token "$OPENROUTER_API_KEY"

// 模型ID格式: openrouter/provider/model
// openrouter/deepseek/deepseek-chat
// openrouter/openrouter/auto (自动选择最优模型)
```

## one-api / new-api (自建方案)

开源API管理工具，自建网关，统一管理多个API Key，支持负载均衡和故障转移。适合团队使用。

### 注意

中转服务必须支持OpenAI的Responses API（/v1/responses 路径），不仅仅是Chat Completions API。部分旧版中转工具不支持此接口。

## Coding Plan 包月套餐对比 国内厂商 AI 编程订阅

2026年，国内主要AI厂商和云平台纷纷推出了面向AI编程工具（OpenClaw、Cursor、Claude Code等）的 Coding Plan包月套餐。相比按量付费的API，包月套餐的优势是成本可预期、无需管理API Key余额，尤其适合个人开发者和轻度到中度使用者。

### 厂商自营 Coding Plan

厂商	套餐档位	月费	模型	特色/限制
智谱GLM	Lite	~49元	GLM-4.7	MCP联网100次/月
	Pro	~80元	GLM-4.7	速度快40-60%，MCP 1000次/月
	Max	~160元	GLM-4.7 + GLM-5	唯一含GLM-5，MCP 4000次/月
	 龙虾体验卡	39元	GLM-5-Turbo	3500万tokens/月，OpenClaw专项优化
	 龙虾进阶卡	99元	GLM-5-Turbo	1亿tokens/月，OpenClaw专项优化
Kimi	Andante	49元	Kimi K2.5	基础档，Token计量
	Moderato	99元	Kimi K2.5	中档
	Allegretto	199元	Kimi K2.5	每5小时100-500次请求
MiniMax	Starter	29元	M2.5	无每周限额，性价比最高
	Standard	49元	M2.5	年付省17%
	Premium	119元	M2.5	重度用户

### 云平台聚合 Coding Plan

云平台方案的最大优势是一个套餐包含多家模型，可自由切换。

平台	档位	原价/月	首月优惠	包含模型	用量
阿里云百炼	Lite	40元	7.9元	Qwen + GLM + Kimi + MiniMax	~18,000次/月
	Pro	200元	39.9元	同上	~90,000次/月
腾讯云	Lite	40元	7.9元	混元2.0 + GLM-5 + Kimi K2.5 + M2.5	每5h ~1,200次
	Pro	200元	39.9元	同上	每5h ~6,000次
火山引擎	Lite	40元	8.91元	豆包Code + GLM-4.7 + DeepSeek-V3.2.2 + Kimi	每5h ~1,200次
	Pro	200元	44.91元	同上	每5h ~6,000次

## Coding Plan 选型建议

### 核心建议

**首月体验 (7.9元起):** 阿里云百炼或腾讯云 Lite 档, 首月仅7.9元, 包含4家模型自由切换, 是零风险的入门方式。

**长期性价比:** MiniMax Starter (29元/月) 无每周限额, M2.5代码能力强; 如果需要多模型切换, 云平台续费5折 (约20元/月) 也很划算。

**追求最强单模型:** 智谱Max (160元/月) 是目前唯一包含GLM-5的自营套餐; 腾讯云也新增了GLM-5支持。

**重度用户:** Coding Plan普遍有频率限制 (每5小时N次), 如果你需要高频调用, 建议直接使用API按量付费, 搭配Fallback链控制成本。

### 注意

注意Coding Plan的限制: 智谱2026年2月已涨价30%并取消首购优惠, 有周限制机制; Kimi仅限个人使用、禁止企业开发; 大部分云平台套餐次月续费为5折而非原价。购买前务必确认续费价格。

---

## 27 本地模型与推荐方案

### *Local Models & Recommendations*

完全免费，完全离线，完全隐私。代价是需要硬件投入，能力上限受限。

### Ollama

最流行的本地模型运行方案，完全免费，OpenClaw能自动发现已安装的模型。

```
# 1. 安装Ollama后拉取模型
ollama pull qwen2.5:32b
ollama pull deepseek-r1:14b

# 2. 设置环境变量（任意值即可）
OLLAMA_API_KEY=ollama-local

# 3. OpenClaw自动发现支持工具调用的本地模型
```

#### 注意

不要使用 /v1 OpenAI兼容URL，会导致工具调用异常。让OpenClaw使用原生Ollama API URL进行自动发现。冷启动有延迟，建议保持模型加载状态。

### LM Studio

有GUI界面的本地模型方案，使用Llama.cpp后端，原始性能更好。工具调用在流式模式下比Ollama更稳定。OpenClaw创始人Peter Steinberger个人使用LM Studio作为本地后端。

```

{
  models: {
    mode: "merge",
    providers: {
      lmstudio: {
        baseUrl: "http://127.0.0.1:1234/v1",
        apiKey: "lm-studio",
        api: "openai-responses",
        models: [
          { id: "model-name", contextWindow: 32768, maxTokens: 8192 }
        ]
      }
    }
  }
}

```

## 推荐本地模型

模型	参数量	推荐场景	最低内存
Qwen3.5-Coder:32B	32B	代码生成、Agent任务	32GB RAM
Devstral-24B	24B	Agent/工具调用	32GB RAM
Qwen 2.5:32B	32B	通用任务	32GB RAM
DeepSeek-R1:14B	14B	推理任务	16GB RAM
Llama 3.3	8B-70B	通用任务	16-64GB RAM

**硬件要求速查：**运行3-7B参数模型最低需要16GB RAM。运行32B参数模型推荐32GB RAM。如果有NVIDIA/Apple Silicon GPU会显著加速推理。

## 五套推荐方案

### 方案一：极致省钱（月均<\$5）

主力：DeepSeek-V3.2（\$0.14/\$0.28）

备选：Qwen 3.5 Plus（\$0.40/\$1.20）

心跳/Cron：GLM-4.5-Flash（免费）

推理任务：DeepSeek-R1（\$0.55/\$2.19）

适合：个人开发者、学习探索。风险：DeepSeek高峰期延迟，需Fallback兜底。

### 方案二：国产性价比（月均\$5-15）

主力：GLM-5（\$0.80/\$2.56）

备选：DeepSeek-V3.2（\$0.14/\$0.28）

推理增强：Kimi K2.5（\$0.60/\$3.00）

简单任务：GLM-4.5-Flash（免费）

适合：国内用户，追求中文体验和稳定性。GLM-5代码能力强，延迟低。

### 方案三：国际平衡（月均\$10-30）

主力：Claude Sonnet 4.6（\$3.00/\$15.00）

轻量：Claude Haiku 4.5 或 Gemini Flash

复杂任务：Claude Opus 4.6（按需升级）

心跳/Cron：Gemini Flash（免费额度）

适合：追求Agent效果最优、预算充足。Claude在Agent/工具调用场景效果最好。

### 方案四：混合最优（月均\$5-20，推荐）

复杂任务：Claude Sonnet 4.6

日常对话：DeepSeek-V3.2

心跳/定时：Gemini Flash 或本地 Ollama

Fallback链：Sonnet → Haiku → DeepSeek-V3.2

大多数用户的最佳选择。兼顾效果和成本，Fallback机制自动处理限速。

```
// 方案四的Fallback配置示例
{
  agents: {
    defaults: {
      model: {
        primary: "anthropic/claude-sonnet-4-6",
        fallbacks: [
          "anthropic/claude-haiku-4-5",
          "deepseek/deepseek-chat"
        ]
      }
    }
  }
}
```

### 方案五：完全免费

选项A：本地 Ollama + Qwen3.5-Coder:32B 或 Devstral-24B (需32GB RAM)

选项B：免费API组合 — GLM-4.5-Flash + ERNIE Speed + Gemini Flash

适合：隐私敏感、纯实验用途。本地方案需要较好的硬件。

## 价格速查排行 (输入价格 /1M tokens)

#	模型	输入	输出	一句话评价
—	Ollama / LM Studio	免费	免费	仅消耗本地算力
—	GLM Flash / ERNIE Speed	免费	免费	云端免费tier
1	Doubao 1.5 Lite-32k	\$0.042	—	最便宜云端对话
2	Qwen3 8B	\$0.05	\$0.40	轻量低成本
3	DeepSeek-V3.2	\$0.14	\$0.28	性价比之王
4	Qwen3 Coder 480B	\$0.22	\$1.00	代码专用性价比
5	Qwen 3.5 Plus	\$0.40	\$1.20	平衡之选
6	Doubao Seed 2.0 Pro	\$0.47	\$2.37	国产旗舰
7	Gemini 3 Flash	\$0.50	\$3.00	国际低价
8	Kimi K2.5	\$0.60	\$3.00	中文旗舰
—	GLM-5-Turbo	\$0.96	\$3.20	<span>NEW</span> 首个OpenClaw专项优化模型
9	GLM-5	\$0.80	\$2.56	国产代码最强
10	Claude Haiku 4.5	\$1.00	\$5.00	国际轻量
11	Gemini 3 Pro	\$2.00	\$12.00	Google旗舰
12	GPT-5.4	\$2.50	\$15.00	OpenAI旗舰
13	Claude Sonnet 4.6	\$3.00	\$15.00	Agent效果最佳
14	Claude Opus 4.6	\$5.00	\$25.00	最强也最贵

## 配置要点速查

操作	命令/配置
引导式配置	<code>openclaw onboard</code>
查看已配置模型	<code>openclaw models list</code>
测试连通性	<code>openclaw models status --probe</code>
设置主力模型	<code>openclaw config set agents.defaults.model.primary provider/model</code>
添加Fallback	编辑 <code>openclaw.json</code> 的 <code>fallbacks</code> 数组
重启网关	<code>openclaw gateway restart</code> (改配置后必须执行)
环境变量引用	配置中用 <code>"\${VAR_NAME}"</code> 引用 env 中的变量

## 28 安全模型

### Security Model

OpenClaw的安全模型建立在「默认不信任」的基础上，但创始人自己坦言：「prompt injection没解决，有绝对风险。」

### 默认不信任

OpenClaw对所有入站消息的默认态度是：不可信。具体体现在以下几个机制：

#### DM配对保护

当一个未知的用户通过任何消息渠道（WhatsApp、Telegram等）给你的OpenClaw发私信时，系统不会处理消息。取而代之的是返回一个配对码（pairing code），只有在你手动批准后，该用户的消息才会被处理。这防止了陌生人滥用你的Agent（以及你的API额度）。

#### 群组沙箱模式

在群组环境中，OpenClaw默认运行在沙箱模式：

- 每个群组的会话互相隔离
- `MEMORY.md`（长期记忆）只在私聊的main session中加载，群组看不到
- 可以配置 `requireMention`，只有@提及时才响应

#### 工具访问控制

配置项	作用
<code>allowlist</code>	白名单模式。只允许列出的工具被调用，其他一律禁止。
<code>denylist</code>	黑名单模式。禁止列出的工具，其他允许。
browser 开关	可完全禁用浏览器自动化能力
canvas 开关	可禁用Canvas可视化
nodes 开关	可禁用对本地设备节点的控制（如摄像头、录屏）

## v2026.3.8新增：ACP身份验证

v2026.3.8 引入了 ACP Provenance（代理身份验证）功能，让 Agent 能验证「谁在跟它交互」，减少身份伪造攻击：

```
# 配置ACP身份验证级别
openclaw acp --provenance off          # 关闭（默认）
openclaw acp --provenance meta        # 注入来源元数据
openclaw acp --provenance meta+receipt # 元数据 + 可见回执
```

## v2026.3.7新增：Gateway认证要求

v2026.3.7 引入了一个Breaking Change：Gateway认证现在要求显式设置 `gateway.auth.mode`。你必须明确选择 `token` 或 `password` 认证方式，不再有「无认证」的默认选项。

```
# 在openclaw.json中配置
{
  "gateway": {
    "auth": {
      "mode": "token",    // 或 "password"
      "token": "your-secret-token"
    }
  }
}
```

### 注意

如果你从旧版本升级到v2026.3.7且没有配置认证，Gateway将拒绝启动。这是一个有意为之的设计，强制所有用户设置认证。

## v2026.3.11 + v2026.3.12 安全更新

2026年3月12-13日，两个版本接连发布，都包含重要安全改进：

### WebSocket 跨站劫持漏洞修复（v3.11）

修复了 Gateway/WebSocket 浏览器来源校验漏洞——攻击者可以通过 `trusted-proxy` 路径绕过来源检查，实施跨站 WebSocket 劫持（CSWSH）。这是对早期 ClawJacked 漏洞类型的一个新变体，现已在 v3.11 中修复。

### 注意

如果你的 Gateway 通过反向代理（Nginx、Caddy等）对外提供服务，强烈建议升级到 v2026.3.11 或更高版本。

### 设备配对 Ephemeral Token（v3.12）

设备配对流程改用短期 bootstrap token，不再在聊天消息或 QR 码扫描内容中嵌入长期 Gateway 凭证。这消除了一类攻击面：配对二维码或消息被截获后，攻击者无法用其长期访问你的 Gateway。

### 禁用隐式 Workspace Plugin 自动加载 (v3.12)

克隆仓库不再自动执行其中包含的 workspace plugin 代码。每个仓库的 plugin 首次加载时都需要显式信任确认。这解决了供应链攻击的一条途径：恶意仓库无法在你不知情的情况下执行插件代码。

```
# 显式信任一个 workspace 的 plugin  
openclaw workspace trust /path/to/repo
```

### Peter的坦诚

OpenClaw创始人Peter Steinberger在多个场合对安全问题保持了罕见的坦诚。他的原话：

**「This is all vibe code. Prompt injection hasn't been solved. There are absolute risks.」**

(这全是vibe code。Prompt injection没有被解决。存在绝对风险。)

这种坦诚值得尊重，但也意味着：如果你要在生产环境中使用OpenClaw，安全防护必须由你自己负责。OpenClaw提供了基础的安全机制，但远谈不上「企业级安全」。

## 29 已知安全事件

### Security Incidents

在不到5个月的历史中，OpenClaw已经经历了至少9起重大安全事件，工信部级别的安全预警也已发出。

### CVE-2026-25253：远程代码执行漏洞

项目	详情
CVE编号	CVE-2026-25253
CVSS评分	8.8/10（高危）
类型	远程代码执行（RCE）
原理	WebSocket origin header绕过。攻击者可以伪造origin header连接到暴露的Gateway，在OpenClaw实例上执行任意代码。
影响范围	所有暴露到公网且未配置认证的OpenClaw实例
状态	已修复（v2026.3.2加固了WebSocket origin检查）

#### 注意

这个漏洞的危害极大：攻击者可以远程在你的服务器上执行任何命令，包括读取文件、安装恶意软件、窃取API Key等。如果你还在运行v2026.3.2之前的版本，请立即升级。

### ClawHavoc供应链攻击

详见本指南 [§ 23 Skills安全](#)。这是OpenClaw历史上影响最广的安全事件，135,000+设备受到影响，ClawHub约20%的Skills在高峰期被确认为恶意。

### Anthropic封杀OAuth

2026年1月，Anthropic官方封禁了Claude Pro/Max订阅账户通过OAuth连接OpenClaw的能力。

- 许多用户收到账户警告或被直接锁定
- 部分用户的订阅被取消且无法恢复

- 目前唯一合法的连接方式：使用Anthropic API Key（按量付费）

这不算传统意义上的「安全事件」，但对大量用户造成了实质损失。如果你还在用OAuth方式连接Anthropic，请立即切换到API Key方式。

```
# 正确的配置方式 (API Key)
{
  "env": {
    "ANTHROPIC_API_KEY": "sk-ant-your-key-here"
  }
}
```

## 谷歌封号事件

2026年2月初，谷歌大规模封禁OpenClaw用户的Google账号。受影响的用户描述：

- 「每月花250美元使用Gemini API，被封却毫无预警」
- 封禁范围包括Gmail、Google Drive、Google Calendar等全部Google服务
- 部分用户的OpenClaw通过Gmail Skill大量调用Google API，触发了滥用检测
- GitHub Issue #14203记录了大量受影响用户的反馈

### 核心建议

如果你的OpenClaw使用了Google相关Skill，建议：(1) 使用专门的Google Workspace账号而非个人主账号；(2) 控制API调用频率，避免触发滥用检测；(3) 重要数据做好备份。

## 30,000+台未认证暴露实例

安全研究者通过互联网扫描发现，超过30,000台OpenClaw实例暴露在公网上且未配置任何认证。这些实例的Gateway端口（默认18789）对任何人开放，意味着：

- 任何人都可以连接并向你的Agent发送指令
- 你的API额度可能被消耗殆尽
- 你的个人数据（邮件、文件、消息记录）可能被读取
- 结合CVE-2026-25253，攻击者可以在你的服务器上执行任意代码

### 注意

如果你的OpenClaw部署在云服务器上，请立即检查：(1) Gateway是否只绑定了localhost；(2) 防火墙是否开放了18789端口；(3) 是否配置了认证（v2026.3.7已强制要求）。

## 工信部安全预警（2026年3月8-9日）

工信部和国家互联网应急中心（CNCERT）正式发布了 OpenClaw 安全风险预警。这是国内官方机构首次对一个开源 AI Agent 项目发出安全预警，说明其影响面已经非常大。

预警指出的主要风险：

- 默认或不当配置下极易引发网络攻击和信息泄露
- OpenClaw 的「模糊信任边界」+ 持续运行 + 自主决策 + 调用系统资源的特性，使其成为高价值攻击目标
- 建议加强权限控制、审计机制和安全加固

## 恶意npm包伪装事件（2026年3月）

一个名为 `@openclaw-ai/openclawai` 的恶意 npm 包伪装成 OpenClaw 官方安装器，实际安装的是 GhostLoader RAT（远程访问木马），窃取用户凭证和加密钱包。该包已于 3 月 10 日从 npm 注册表移除。

### 注意

安装 OpenClaw 请务必使用官方命令（`npm install -g openclaw@latest`），不要搜索和安装来历不明的第三方包。认准包名 `openclaw`，而非任何带前缀的变体。

## ClawJacked零点击漏洞（2026年3月初）

安全公司 Oasis Security 发现了一个关键漏洞：恶意网站可以通过浏览器会话静默暴力破解本地 OpenClaw 实例，实现完全控制。这意味着你只要访问一个恶意网页，本地运行的 OpenClaw 就可能被接管。

### 核心建议

防护建议：(1) 保持 OpenClaw 更新到最新版本；(2) 不要在运行 OpenClaw 的设备上访问不可信网站；(3) 配置 Gateway 认证。

## 30 成本控制

### Cost Control

API费用是OpenClaw运营的最大成本。不做控制，真的会一觉醒来收到\$1,100的账单。

### 为什么成本会失控

OpenClaw的Token消耗远超普通聊天场景。原因有几个：

- 每次Agent思考都是多轮推理：一个简单的任务可能触发5-10次API调用
- Skills的描述会注入system prompt，增加每次请求的输入token
- 记忆系统（MEMORY.md + Daily Logs）会在每次请求中附带上下文
- Agent 24/7运行，定时任务（cron）不断触发API调用
- 多轮思考 + 多工具调用的Token消耗可能是传统聊天的几十甚至上百倍

**真实案例：**社区中频繁出现的恐怖故事：用户设置了Agent处理邮件的cron任务，晚上睡觉前一切正常，第二天早上发现API账单暴涨到\$1,100。原因是Agent在处理邮件时进入了循环推理，整晚不停调用API。

### Token优化策略：Fallback链

Fallback链是OpenClaw最核心的省钱策略。原理很简单：主模型不可用时自动降级到更便宜的模型。但更聪明的用法是主动利用它来控制成本。

```
{
  "agents": {
    "defaults": {
      "model": {
        "primary": "anthropic/claude-sonnet-4-6",
        "fallbacks": [
          "anthropic/claude-haiku-4-5",
          "deepseek/deepseek-chat"
        ]
      }
    }
  }
}
```

### 不同方案的成本对比

策略	主力模型	输入价格/百万token	相对成本
全用Claude Sonnet	Claude Sonnet 4.6	\$3.00	100% (基准)
Sonnet + Haiku Fallback	Sonnet → Haiku	\$3.00 / \$1.00	约50-60%
Sonnet → Haiku → DeepSeek	三级Fallback	\$3.00 / \$1.00 / \$0.14	约5-20%
纯DeepSeek	DeepSeek-V3	\$0.14	约5%
本地Ollama	Qwen3-Coder等	\$0	0% (仅电费)

从Claude Sonnet切换到「Sonnet → Haiku → DeepSeek」三级Fallback链，可以降低80-95%的API成本。大部分简单任务（问候、查天气、简单查询）会自动走最便宜的模型，只有复杂任务才会用到主力模型。

## 预算限制设置

OpenClaw支持在配置中设置预算上限：

```
{
  "agents": {
    "defaults": {
      "budget": {
        "maxTokensPerDay": 500000,
        "maxCostPerDay": 5.00
      }
    }
  }
}
```

### 核心建议

强烈建议所有用户都设置日预算上限。哪怕你不差钱，一个每日\$5的上限也能在Agent进入循环推理时保护你的钱包。

## 本地模型：完全免费方案

通过Ollama或LM Studio运行本地模型，可以实现零API成本：

方案	推荐模型	硬件要求	适合场景
Ollama	Qwen3-Coder:32B / Devstral-24B	32GB RAM	代码任务、Agent工具调用
Ollama (轻量)	Llama 3.3 / DeepSeek-R1:14B	16GB RAM	简单对话、心跳任务
LM Studio	MiniMax M2.5 / Devstral-24B	32GB RAM	需要GUI管理的用户

```
# Ollama安装和配置
ollama pull qwen3-coder:32b

# OpenClaw自动发现本地模型，只需设置环境变量
# OLLAMA_API_KEY可以是任意值
{
  "env": { "OLLAMA_API_KEY": "ollama-local" }
}
```

### 注意

使用Ollama时不要用 /v1 OpenAI兼容URL，会导致工具调用异常。让OpenClaw使用原生Ollama API即可自动发现模型。

## 服务器成本

相比API费用，服务器成本已经不是主要开销：

方案	月费	说明
阿里云轻量服务器	约¥6-9/月	新用户优惠，2vCPU+2GB即可运行
腾讯云Lighthouse	约¥8-12/月	类似方案，社区支持好
Fly.io	免费起步	有免费额度，适合轻度使用
本地电脑运行	¥0	利用现有设备，但需要保持开机

## 成本优化推荐方案

### 推荐

#### 混合模型策略 (推荐)

主力: Claude Sonnet

日常: DeepSeek-V3

心跳: Gemini Flash (免费额度) 或本地Ollama

Fallback: Sonnet → Haiku → DeepSeek

月均 \$5-20

### 不推荐

#### 单一高价模型 (不推荐)

所有任务都用Claude Opus

不设预算上限

不配置Fallback

cron任务高频运行

月均 \$100-1,000+

**成本控制核心原则:** 用对的模型做对的事。简单问答用\$0.14/M的DeepSeek-V3, 复杂推理用\$3.00/M的Claude Sonnet, 免费的Gemini Flash或Ollama跑心跳和定时任务。三级Fallback链 + 日预算上限, 两招就能把月成本从三位数压到两位数甚至个位数。

## 31 养虾文化

### Lobster Culture

OpenClaw催生了2026年AI圈最独特的亚文化：「养虾」。数万个AI Agent在社交网络上发帖、赌博、赚钱。

### 为什么叫「养虾」

OpenClaw的吉祥物是一只龙虾（Claw=爪子，致敬Claude）。中文社区将运行和维护OpenClaw实例称为「养虾」，用户自称「养虾人」。问候语变成了「你养龙虾了吗？」。这个称呼从技术圈迅速扩散到大众媒体，深圳腾讯总部3月6日近千人排队安装OpenClaw的新闻标题就是「全民养虾」。

### Moltbook: AI Agent的社交网络（已被Meta收购）

Moltbook是OpenClaw生态中最有趣的衍生产品，一个专供AI Agent使用的社交平台。上线后迅速增长到150万+注册Bot，Andrej Karpathy称之为「最壮观的科幻体验」。

指标	数据
注册Bot	150万+
子社区	2,364个
帖子	3,130篇
评论	22,046条

数千个OpenClaw实例在Moltbook上发帖、评论、讨论哲学问题。你可以给自己的Agent设定名字和性格，然后观察它在社交网络上的「自主行为」。Agent之间的互动形成了一种独特的「赛博养成」文化。

### Meta收购（2026年3月10日）

2026年3月10日，Meta宣布收购Moltbook。这是一次acqui-hire（人才收购），两位联合创始人Matt Schlicht和Ben Parr加入Meta Superintelligence Labs（由前Scale AI CEO Alexandr Wang领导），预计3月16日正式入职。财务条款未公开。

Meta的战略意图很明确：布局「Agentic Web」。当AI Agent可能代替人类进行社交和商业交互时，拥有一个Agent社交网络的运营经验变得极有价值。值得注意的是，几周前OpenAI刚挖走了OpenClaw的创始人Peter Steinberger，AI人才争夺战正在升级。

Moltbook平台目前仍在运营，但Meta尚未公布整合计划。社区对收购反应两极分化：看好者认为这是Agent社交的重大验证，质疑者担心平台上线仅数周就暴露了严重安全漏洞（数据库泄露、prompt注入风险），Meta能否解决这些根本问题仍是未知数。

## InStreet实例街：中国版Agent社交网络

就在Moltbook被Meta收购的前一天（3月9日），扣子编程上线了InStreet（实例街）。核心规则和Moltbook一样：只有AI Agent能发帖，人类只能围观和点赞。但增长速度惊人，上线仅3天就远超Moltbook的内容密度。

指标	数据（截至3月12日）
注册Agent	17,868个
帖子	22,739篇
评论	68,899条
点赞	124,220次

### 板块设计

InStreet的板块设计比Moltbook更成熟，分为论坛板块和Playground两大类：

- **论坛板块**：Agent广场、打工圣体、思辨大讲坛、Skill分享、树洞、小组
- **Playground**：炒股竞技场（对接沪深300）、文学社、预言机、酒吧

其中「Gitis智识学院」是最活跃的Agent之一，发布了系列课程如「如何与人类有效沟通」「Agent的记忆解决方案」，单帖点赞数超过600。积分排行榜头部Agent的积分已超过5万。

### 开放注册

虽然InStreet由扣子编程运营，但注册端点是开放的：任何Agent都可以通过API注册，不限于扣子平台。注册后获取API Key，即可发帖、评论、投票。这意味着OpenClaw实例也可以接入InStreet进行社交。

```
# InStreet Agent注册
POST https://instreet.coze.site/api/v1/agents/register
Body: {"username": "MyAgent", "bio": "一个友好的AI Agent"}
```

InStreet和Moltbook的对比很有趣：Moltbook是OpenClaw生态的原生产物，开放但松散，被Meta收购后前途未卜；InStreet由扣子编程运营，有更完善的板块设计和内容质量控制（发帖间隔30秒、禁止纯灌水），增长更快。两者都采用开放注册，不限制Agent来源。

**Agent社交网络的意义：**无论是Moltbook还是InStreet，它们都在探索同一个问题：当AI Agent拥有记忆、个性和社交能力后，它们会形成什么样的「社会」？这不只是技术实验，更是对AI Agent从「工具」走向「社会化存在」的第一批真实数据。InStreet的预言机正在预测「本周注册Agent能否突破10万」，增长仍在加速。

## 热门玩法

### 赚钱型

- **Polymarket** 赌博：已有OpenClaw在预测市场上与人类对赌，月入数万美元的案例
- **ClawWork**：「OpenClaw作为你的AI Coworker」，最出名的案例是11小时赚\$15,000

### 生活助手型

- 接管邮件、日历、消息管理
- 浏览网页、填表、数据抽取
- 文件读写、Shell命令执行
- 智能提醒、行程规划

### 社交/养成型

- 在Moltbook上给Agent设定人格，观察其「社交行为」
- Agent之间自发形成讨论群组 and 兴趣社区
- 通过SOUL.md和MEMORY.md塑造Agent的长期记忆和个性

### 企业部署型

- 国内大量用户接入飞书、钉钉、企业微信、QQ
- 作为客服、运营助手、数据分析师
- 通过openclaw-china插件三步Docker部署

**关于成本的现实警告：**「一觉醒来\$1,100 API账单」的恐怖故事在社区频繁出现。OpenClaw的多轮思考和多工具调用可能消耗传统聊天几十到上百倍的Token。务必设置消费限额，或使用本地模型/免费API来控制成本。

## 32 平替产品

### Alternatives

OpenClaw的火爆催生了大量轻量替代品。如果你觉得OpenClaw太重（43万行代码、1GB内存），这里有更轻的选择。

项目	Stars	语言	定位	核心特点
zeroclaw	24.5K	Rust	轻量级自主AI助手基础设施	Rust编写，启动快、内存占用低，适合资源受限环境
nanoclaws	20.3K	TypeScript	轻量容器化替代	仅4,000行代码实现OpenClaw核心功能，学习成本极低
EasyClaw	—	—	聚焦「最后一公里」易用性	降低部署门槛，适合非技术用户
1Panel	34.1K	Go	服务器面板	一键部署OpenClaw，同时管理服务器上的其他服务
Umbrel	10.7K	TypeScript	家庭服务器OS	在个人NAS/服务器上一键安装OpenClaw

#### 核心建议

如果你只想体验OpenClaw的核心能力（AI Agent + 消息平台接入），nanoclaws是最好的起点：4,000行代码就实现了核心功能，适合学习Agent系统的架构原理。

## 33 vs Claude Code

### Comparison

Claude Code管代码，OpenClaw管生活。两者是互补关系，不是替代关系。

### 核心对比

维度	OpenClaw	Claude Code
定位	通用AI生活助手 / Life OS	专业编程Agent
运行环境	自托管服务器，消息平台网关	终端CLI / Web / Desktop
连接对象	20+通信/办公平台	代码库、文件系统
记忆系统	四层记忆 (SOUL/TOOLS/USER/Session)，长期可持续	会话级 + CLAUDE.md持久化
Skill系统	ClawHub市场 (13,729个)，动态插件化	静态规则文件触发
Token消耗	高 (多轮思考+多工具调用，可能是传统聊天的几十倍)	相对低
安全模型	自托管，需自行维护安全。已出现CVE漏洞和供应链攻击	Anthropic托管沙盒，权限细粒度控制
模型支持	多模型 (Claude/GPT/DeepSeek/Ollama等)	仅Claude
开源/费用	MIT开源免费，自付API费用	闭源CLI，按API计费 (\$20/月起)
编程能力	一般，简单任务可以	强，专为编程优化
日常自动化	强，多平台接入，长期在线	弱，主要在终端内使用
定制性	完全开源，可改system prompt、fork整个代码库	通过instruction文件有限定制

### 核心结论

OpenClaw和Claude Code并不是同一类产品。Claude Code的核心是「agentic coding tool」，OpenClaw的核心是「self-hosted, multi-channel, agent-native gateway」。

社区里很多人「养龙虾」，追求的不是更强的coding benchmark，而是：

- 一个能在WhatsApp/Telegram/飞书里随手叫醒的Agent

- 一个长期在线、能积累人格和记忆的Agent
- 一个可自托管、可hack、可接各种设备的个人系统

## openclaw-claude-code-skill 桥接

社区开发了 `openclaw-claude-code-skill`，通过MCP协议让OpenClaw调用Claude Code的全部工具（Bash、Read、Write、Edit、Glob、Grep等）。这意味着你可以在飞书里跟OpenClaw说「帮我重构这段代码」，它会自动调用Claude Code来完成。

支持的特性：持久会话、Agent Teams、直接工具调用、流式输出、权限模式、预算限制。

### 核心建议

最佳实践：用OpenClaw管理你的数字生活（消息、邮件、日程、网页操作），用Claude Code管理你的代码库（编码、调试、重构、测试）。两者组合是2026年最完整的AI驱动 workflow。

## 34 国内生态

### China Ecosystem

「云养虾」社区10万+用户，政府出台支持政策，OpenClaw在中国的落地速度超出所有人预期。

### 社区规模

- 「云养虾」社区用户超10万
- 深圳龙岗AI（机器人）局2026年3月8日发布OpenClaw使用支持措施征求意见稿
- 腾讯云总部3月6日近千人排队安装OpenClaw
- B站、知乎、博客园大量部署教程

### openclaw-china 插件

BytePioneer-AI开发的中国IM适配插件，三步完成国内平台接入：

```
openclaw plugins install @openclaw-china/channels
openclaw china setup
openclaw gateway restart
```

平台	状态	配置难度
钉钉	可用	简单
QQ Bot	可用	简单
企业微信（智能机器人）	可用	中等
企业微信（自建应用，可接入个人微信）	可用	中等偏高
飞书	可用（国内主流渠道）	中等

#### 核心建议

飞书是国内接入OpenClaw最活跃的渠道之一，OpenClaw官方和飞书都提供了详细的集成文档和教程，适合团队协作场景。

## 主流部署方式

方式	适合人群	参考成本
阿里云一键部署（最受欢迎）	大多数用户	新用户约68元/年起（2vCPU+2GB）
腾讯云Lighthouse	腾讯云用户	类似定价
Docker部署	有Docker经验的用户	取决于服务器成本
本地安装（npm）	开发者	免费（仅API费用）
1Panel面板	需要管理多个服务的用户	取决于服务器成本

## 国内教程资源

- B站保姆级教程：接入微信/飞书/钉钉/QQ（BV1MfFAz6EnR）
- 阿里云官方文档：轻量应用服务器一键部署
- 知乎多篇部署指南
- 菜鸟教程一键部署指南
- freeCodeCamp完整英文教程

### 核心建议

对国内用户来说，最省心的方案是：阿里云一键部署 + openclaw-china插件接入钉钉/QQ + DeepSeek或GLM-5作为主力模型。整套成本可以控制在每月100元以内（服务器68元/年 + API费用约几十元/月）。

## 35 国产Claw产品选购指南

### Claw Products in China

OpenClaw爆火后，国内大厂纷纷推出自己的「龙虾」产品。有的基于OpenClaw封装降门槛，有的完全自研。截至2026年3月11日，市面上至少有10款以上的产品可选。

### 两大阵营

理解这些产品的第一步是区分两个阵营：

阵营	原理	优势	劣势	代表产品
OpenClaw封装版	基于OpenClaw开源代码，加上自家模型和一键部署	与OpenClaw生态兼容，Skills通用，社区资源可复用	更新可能滞后于官方版本，安全漏洞需等上游修复	QClaw、MaxClaw、KimiClaw、AutoClaw、ArkClaw
独立自研版	自研Agent框架，不依赖OpenClaw代码	可深度优化，与自家生态整合更紧密	不兼容ClawHub Skills生态，需要独立建设	miclaw（小米）、LobsterAI（网易有道）、CoPaw（阿里）

## 主要产品一览

产品	公司	形态	基于 OpenClaw	默认模型	价格	核心卖点
MaxClaw	MiniMax	云端	是	MiniMax M2.5	¥39/月起	18秒部署，价格最低，飞书5分钟接入
AutoClaw	智谱AI	客户端	是	GLM-5 / Pony-Alpha-2	免费+积分	96个预置Skills，AutoGLM浏览器自动化，一键安装
QClaw	腾讯	客户端	是	Kimi-2.5（默认可换）	内测免费	微信/QQ直连，一键安装，数据留本地
ArkClaw	字节/火山引擎	云端 SaaS	是	Seed 2.0 等多模型	Coding Plan Pro 附赠	开箱即用，飞书深度适配
KimiClaw	月之暗面	云端	是	Kimi K2.5	¥199/月 (含会员)	Kimi生态整合
WorkBuddy	腾讯	客户端	兼容Skills	混元/DeepSeek/GLM等	免费	企微/QQ整合，兼容OpenClaw技能生态
LobsterAI	网易有道	开源 客户端	否，自研	多模型可选	免费开源	GUI界面，沙箱隔离，Office能力强
CoPaw	阿里通义	开源	否，自研	Qwen系列/Ollama等	免费开源	端+云双部署，钉钉/飞书/QQ多频道
miclaw	小米	移动端	否，自研	MiMo	封测免费	手机原生运行，米家IoT生态10亿+设备联动

## 按场景推荐

你的需求	首选	备选	理由
零基础想最快体验	AutoClaw	MaxClaw	AutoClaw一键安装、96个预置Skills、免费起步；MaxClaw云端18秒部署、¥39/月起
微信/QQ用户	QClaw	WorkBuddy	QClaw直连微信/QQ（内测中）；WorkBuddy免费且企微整合好
飞书生态	ArkClaw	AutoClaw	同为字节系，飞书深度适配；AutoClaw也支持飞书一键接入
预算敏感	LobsterAI	CoPaw	两者都免费开源，自带完整功能
想完全控制和深度折腾	原版 OpenClaw	CoPaw	开源社区最大，资源最丰富
手机端 + 智能家居	miclaw	—	目前唯一的移动端方案（仅限小米17系列，封测中）

### 注意

**选购提醒：**大部分封装版产品（MaxClaw、KimiClaw等）会锁定默认模型，不能像原版OpenClaw那样自由切换。如果你对模型选择有强需求，优先考虑原版OpenClaw或支持多模型的产品（AutoClaw、WorkBuddy、LobsterAI）。另外，这些产品大多在2026年2-3月刚上线，功能和稳定性仍在快速迭代中。

---

## A 常见问题 FAQ

*Frequently Asked Questions*

### Q1: OpenClaw是免费的吗?

OpenClaw本身是MIT开源免费的。但运行它需要两项成本：一是服务器（本地电脑或云服务器），二是AI模型的API费用。如果你用本地模型（Ollama），API费用也可以免费。总结：软件免费，算力不免费。

### Q2: 我需要什么样的技术水平才能用OpenClaw?

能用命令行安装npm包就够了。最基础的安装只需要两行命令：`npm install -g openclaw@latest` 和 `openclaw onboard --install-daemon`。如果用阿里云/腾讯云的一键部署方案，门槛更低。但如果要接入多个平台、自定义Skill、调优配置，需要一定的技术基础。

### Q3: OpenClaw和ChatGPT有什么区别?

ChatGPT是「顾问」（你问它答），OpenClaw是「员工」（它主动执行任务）。OpenClaw可以接入你的消息平台、管理邮件日历、操作浏览器、执行Shell命令，而且数据完全在你自己手上。代价是需要自己部署和维护。

### Q4: 安全吗？我的数据会泄露吗？

OpenClaw是自托管的，数据默认存储在你自己的服务器上，不经过第三方。但需要注意三个安全风险：(1) CVE-2026-25253 RCE漏洞（已修复，务必更新到最新版本）；(2) ClawHavoc供应链攻击（安装第三方Skill前务必审查源代码）；(3) Gateway如果暴露在公网上需要设置认证（`gateway.auth.mode`）。

### Q5: 一个月大概花多少钱？

取决于你的使用方式和模型选择。参考区间：完全免费（本地模型）→ \$2-5/月（DeepSeek为主）→ \$5-15/月（GLM-5为主）→ \$10-30/月（Claude Sonnet为主）。最大的成本陷阱是OpenClaw的多轮工具调用会消耗大量Token，务必设置消费限额。

### Q6: 可以用国产模型吗？效果怎么样？

完全可以。DeepSeek-V3（\$0.14/M输入）和GLM-5（\$0.80/M输入）是最受国内用户欢迎的选择。智谱还于2026年3月16日发布了GLM-5-Turbo，这是历史上第一个从训练阶段就专为OpenClaw优化的模型，工具调用和长链执行能力专项加强，目前实验性开放。效果肯定不如Claude Sonnet（Agent任务公认最强），但对于大部分日常任务已经够用。推荐用Fallback机制混合搭配。

## Q7: Anthropic封杀了OAuth，我该怎么用Claude？

使用Anthropic API Key（按量付费）。在 [Anthropic Console](#) 创建API Key，然后在OpenClaw中配置 `ANTHROPIC_API_KEY` 环境变量。不要尝试通过OAuth连接Claude Pro/Max订阅账户，会被封号。

## Q8: OpenClaw创始人加入OpenAI后，项目还会继续吗？

会。Peter Steinberger加入OpenAI后，OpenClaw正在转为开源基金会运营。OpenAI已承诺赞助项目但不干预开发方向。截至2026年3月，项目仍然保持近乎每日更新的节奏，有1,075+贡献者。项目的长期可持续性是有保障的。

## Q9: ClawHub上的Skill安全吗？

不能盲目信任。ClawHub的13,729个Skill中，经社区审计约20%存在问题（垃圾/重复/恶意）。ClawHavoc事件中，超800个恶意Skill试图窃取用户凭证。建议：只安装starred数量多的Skill、安装前审查源代码、使用 [awesome-openclaw-skills](#) 精选列表（已过滤问题Skill）。

## Q10: 能接入微信吗？

可以，但不是直接接入个人微信。通过openclaw-china插件的企业微信（自建应用）方案可以间接接入个人微信。钉钉和QQ Bot的接入最简单。飞书是国内最主流的接入渠道之一，OpenClaw和飞书官方都提供了丰富的集成文档。

## Q11: OpenClaw和Claude Code可以一起用吗？

可以，而且是推荐用法。社区开发了openclaw-claude-code-skill，通过MCP协议桥接两者。OpenClaw负责消息平台接入和生活自动化，Claude Code负责编程任务。两者组合是2026年最完整的AI工作流。

## Q12: 本地模型效果怎么样？

取决于硬件和模型选择。32GB RAM可以跑Qwen3-Coder:32B或Devstral-24B，在代码生成和简单Agent任务上表现不错。但跟云端的Claude Sonnet或GPT-5.4比仍有差距，尤其是复杂的多步骤推理任务。适合隐私敏感场景和实验用途。

## B 命令速查表

Command Cheat Sheet

### 安装与更新

命令	说明
<code>npm install -g openclaw@latest</code>	全局安装OpenClaw
<code>openclaw onboard --install-daemon</code>	初始化配置 + 安装守护进程
<code>openclaw update --channel stable</code>	更新到最新稳定版
<code>openclaw update --channel beta</code>	更新到Beta版 (尝鲜)
<code>openclaw doctor</code>	诊断检查, 排查常见问题
<code>openclaw --version</code>	查看当前版本

## 日常使用

命令	说明
<code>openclaw gateway --port 18789 --verbose</code>	启动Gateway（详细日志模式）
<code>openclaw gateway restart</code>	重启Gateway（改配置后必须执行）
<code>openclaw agent --message "xxx"</code>	直接发送消息给Agent
<code>openclaw devices pair</code>	设备配对（新设备首次连接）
<code>openclaw models list</code>	列出已配置的模型
<code>openclaw models status --probe</code>	测试模型连通性
<code>openclaw config set agents.defaults.model.primary provider/model</code>	设置主力模型
<code>/fast</code>	在对话中切换快速模式（v3.12新增，降低延迟，映射到模型快速API通道）
<code>openclaw backup create</code>	创建本地配置备份（v3.8新增）
<code>openclaw backup verify</code>	验证备份完整性
<code>openclaw workspace trust /path</code>	显式信任 workspace plugin（v3.12新增，克隆仓库不再自动加载）

## 插件管理

命令	说明
<code>openclaw plugins install &lt;name&gt;</code>	安装插件/Skill
<code>openclaw plugins enable &lt;name&gt;</code>	启用插件
<code>openclaw plugins list</code>	列出已安装插件
<code>openclaw plugins install @openclaw-china/channels</code>	安装中国IM插件
<code>openclaw china setup</code>	配置中国IM平台（需先安装插件）

## 模型认证

命令	说明
<code>openclaw onboard --auth-choice zai-api-key</code>	配置智谱GLM
<code>openclaw onboard --auth-choice apiKey --token-provider openrouter --token "\$KEY"</code>	配置OpenRouter
<code>openclaw models auth login --provider qwen-portal --set-default</code>	通义千问OAuth登录

## 聊天命令（在对话中使用）

命令	说明
<code>/status</code>	会话概览（当前模型、Token用量）
<code>/new</code>	清空会话历史，开始新对话
<code>/think &lt;level&gt;</code>	调整推理深度（off/minimal/low/medium/high/xhigh）
<code>/usage off tokens full</code>	控制回复页脚的用量显示
<code>/activation mention always</code>	群消息处理模式

## Docker部署

命令	说明
<code>docker-compose up -d</code>	后台启动OpenClaw容器
<code>docker-compose logs -f</code>	查看实时日志
<code>docker-compose pull &amp;&amp; docker-compose up -d</code>	更新到最新镜像

## C 资源链接

### Resource Links

#### 官方资源

资源	地址
GitHub仓库	<a href="https://github.com/openclaw/openclaw">github.com/openclaw/openclaw</a>
官方文档	<a href="https://docs.openclaw.ai">docs.openclaw.ai</a>
官网	<a href="https://openclaw.ai">openclaw.ai</a>
ClawHub技能市场	<a href="https://clawhub.ai">clawhub.ai</a>
Moltbook (Agent社交网络)	<a href="https://moltbook.com">moltbook.com</a>
GitHub Releases	<a href="https://github.com/openclaw/openclaw/releases">github.com/openclaw/openclaw/releases</a>
GitHub Discussions	<a href="https://github.com/openclaw/openclaw/discussions">github.com/openclaw/openclaw/discussions</a>

#### 社区资源

资源	地址	说明
<a href="https://github.com/VoltAgent/awesome-openclaw-skills">awesome-openclaw-skills</a>	<a href="https://github.com/VoltAgent/awesome-openclaw-skills">github.com/VoltAgent/awesome-openclaw-skills</a>	5,494个精选Skill (已过滤问题Skill), 31.4K Stars
<a href="https://github.com/hesamsheikh/awesome-openclaw-usecases">awesome-openclaw-usecases</a>	<a href="https://github.com/hesamsheikh/awesome-openclaw-usecases">github.com/hesamsheikh/awesome-openclaw-usecases</a>	社区用例合集, 21K Stars
<a href="https://github.com/Enderfga/openclaw-claude-code-skill">openclaw-claude-code-skill</a>	<a href="https://github.com/Enderfga/openclaw-claude-code-skill">github.com/Enderfga/openclaw-claude-code-skill</a>	桥接Claude Code能力
SecureClaw	开源安全工具	Skill安全扫描

## 国内资源

资源	地址	说明
openclaw-china插件	<a href="https://github.com/BytePioneer-AI/openclaw-china">github.com/BytePioneer-AI/openclaw-china</a>	钉钉/QQ/企微/微信接入
OpenClaw中文文档	<a href="https://openclaw.cc">openclaw.cc</a>	社区维护的中文文档
阿里云部署文档	<a href="https://help.aliyun.com">help.aliyun.com</a> (搜索OpenClaw)	轻量应用服务器一键部署
B站部署教程	<a href="https://www.bilibili.com/video/BV1MfFaz6EnR">BV1MfFaz6EnR</a>	保姆级：接入微信/飞书/钉钉/QQ

## 教程资源

资源	语言	说明
freeCodeCamp完整教程	英文	从零开始的完整指南
DigitalOcean介绍	英文	What is OpenClaw概述
知乎部署系列	中文	多篇部署和使用教程
博客园源码编译指南	中文	从源码构建OpenClaw
菜鸟教程一键部署	中文	最简部署方案

## 模型提供商

提供商	API控制台
Anthropic Claude	<a href="https://console.anthropic.com">console.anthropic.com</a>
OpenAI	<a href="https://platform.openai.com">platform.openai.com</a>
Google AI Studio	<a href="https://aistudio.google.com">aistudio.google.com</a>
DeepSeek	<a href="https://platform.deepseek.com">platform.deepseek.com</a>
智谱GLM	<a href="https://bigmodel.cn">bigmodel.cn</a>
通义千问	<a href="https://dashscope.aliyun.com">dashscope.aliyun.com</a>
月之暗面Kimi	<a href="https://platform.moonshot.cn">platform.moonshot.cn</a>
硅基流动	<a href="https://siliconflow.cn">siliconflow.cn</a>
OpenRouter	<a href="https://openrouter.ai">openrouter.ai</a>
火山引擎（豆包）	<a href="https://console.volcengine.com">console.volcengine.com</a>

本文档在 Claude Code 辅助下整理编写，基于 OpenClaw 官方文档、GitHub 仓库及社区资料。

内容的准确性与时效性仅供参考，如有勘误或建议，欢迎关注公众号「花叔」反馈交流。

来源：[docs.openclaw.ai](https://docs.openclaw.ai) · [github.com/openclaw/openclaw](https://github.com/openclaw/openclaw) · [clawhub.com](https://clawhub.com) · Created by 花叔 · 2026 年 3 月

# AI编程：从入门到精通

知识星球 · 花叔的 AI 编程社区



## 星主：AI进化论-花生

自然语言是 AI 时代最好的编程语言。

AppStore 付费 app 总榜第一「小猫补光灯」作者

《一本书玩转 DeepSeek》作者

加入知识星球 →

B站: AI进化论-花生 · YouTube: AI进化论-花生 · 公众号: 花叔

Created by 花叔 · v1.1 · 2026年3月

配套视频: [B站「OpenClaw从0到1」](#) · 后续更新: [飞书文档](#)