

# MCP và AI agent

Cánh cửa vào thế giới **MCP và AI agent**, giúp bạn xây dựng các hệ thống thông minh, linh hoạt.

- Giới thiệu
  - Giới thiệu
  - MCP Là Gì

# Giới thiệu

Giới thiệu

# Giới thiệu

## Mục Tiêu

Đến cuối khóa học, bạn sẽ:

- Hiểu rõ các nguyên tắc cốt lõi của MCP** – Nắm vững cách thức hoạt động và triết lý đằng sau giao thức này.
- Xây dựng server MCP** – Tự phát triển server MCP từ đầu hoặc tích hợp các server có sẵn.
- Triển khai MCP client** – Kết nối client với server để tạo ra các quy trình AI mạnh mẽ.
- Xây dựng các workflow AI tiên tiến** – Ứng dụng MCP vào các tác vụ phức tạp như tự động hóa, xử lý ngôn ngữ tự nhiên và tương tác đa tác nhân (multi-agent).
- Debug và giám sát hệ thống** – Học cách kiểm tra, ghi log, theo dõi hiệu suất và đảm bảo an ninh cho hệ thống MCP.

Khóa học cũng sẽ đề cập đến các yếu tố quan trọng trong phát triển phần mềm như **testing, logging, monitoring, security**, cùng các tình huống thực tế để bạn sẵn sàng áp dụng vào dự án thực tế.

## Đối Tượng

Cuốn sách này được thiết kế chủ yếu cho:

- Lập trình viên và kỹ sư phần mềm** muốn tìm hiểu về MCP.
- Nhà khoa học dữ liệu** quan tâm đến việc tích hợp AI vào hệ thống.
- Những người **có kinh nghiệm lập trình cơ bản**, dù không phải là kỹ sư chuyên nghiệp.

Một số học viên bất ngờ như **luật sư, bác sĩ** cũng đã tham gia và hoàn thành khóa học thành công. Tuy nhiên, khóa học **không dành cho người mới bắt đầu hoàn toàn**.

## Yêu Cầu Kiến Thức Trước Khi Học

Để theo kịp nội dung, bạn cần:

- Kinh nghiệm lập trình Python** (viết hàm, class, chạy chương trình).
- Hiểu biết cơ bản về Git** (clone, commit).

- **Quen thuộc với môi trường ảo (virtual environment)** và cách thiết lập biến môi trường.
- **Kiến thức cơ bản về phát triển ứng dụng AI** (RAG, agent, ReAct framework).

Khóa học sẽ hướng dẫn từng bước, nhưng **không giải thích lại kiến thức Python cơ bản**. Nếu bạn chưa tự tin, hãy ôn tập trước để tận dụng tối đa nội dung.

# MCP Là Gì

## MCP Là Gì Và Tại Sao Nó Đang "Hot"?

Hôm nay chúng ta sẽ nói về **MCP (Model Context Protocol)**, một giao thức đang được bàn tán rất nhiều trong cộng đồng AI, đặc biệt là trên **ECS (Anthropic's Ecosystem)**.

Hiện nay, **MCP đang được áp dụng rộng rãi** trong nhiều ứng dụng như **Cursor, Cloud AI**, và hàng loạt nền tảng khác. Mục tiêu của bài viết này là giúp bạn hiểu rõ:

- Cách MCP hoạt động
- Tại sao nó quan trọng trong phát triển AI agent
- Làm thế nào để xây dựng và tích hợp MCP server

## Bài Toán MCP Giải Quyết: "Tích Hợp Một Lần, Chạy Mọi Nơi"

Hãy tưởng tượng bạn đang xây dựng một **AI agent** có khả năng:

- Gửi tin nhắn Slack
- Đọc/gửi email (Gmail API)
- Truy vấn cơ sở dữ liệu

Thông thường, bạn sẽ phải:

1. **Tự code tích hợp từng API** (Slack, Gmail, DB).
2. **Giới hạn quyền truy cập** (ví dụ: không cho agent xóa email).
3. **Đóng gói thành "tools"** để agent sử dụng.

Vấn đề phát sinh khi:

- **Agent của bạn thành công** và người khác muốn sử dụng nó trong **nhiều nền tảng khác nhau** (Cursor, Windsurf, Lovable, GitHub Copilot...).
- Mỗi nền tảng yêu cầu **một phiên bản tích hợp riêng** → Bạn phải viết lại code nhiều lần!

## Giải Pháp: Thêm Một Lớp Trừu Tượng (Abstraction Layer)

Đây là lúc **MCP xuất hiện**! Thay vì phải tích hợp riêng lẻ với từng agent, bạn chỉ cần:

1. **Xây dựng một MCP server** chứa các chức năng (Slack, Gmail, DB...).
2. **Các agent hỗ trợ MCP** (Cursor, Windsurf...) sẽ tự động kết nối đến server của bạn mà không cần chỉnh sửa thêm.

### Ví dụ thực tế:

- Bạn phát triển một **AI email assistant** trên Cursor.
- Nhờ MCP, nó có thể chạy ngay trên **Windsurf, GitHub Copilot** mà không cần viết thêm code!

## MCP Giống Như Mạng Xã Hội - Càng Nhiều Người Dùng, Càng Mạnh

Tương tự **Facebook, Twitter**, giá trị của MCP nằm ở **mạng lưới người dùng**:

- **Càng nhiều MCP server & agent tương thích** → Khả năng kết nối càng rộng.
- **Cộng đồng phát triển mạnh** → Xuất hiện nhiều công cụ mở rộng (pre-built servers, plugins...).

## MCP Hoạt Động Như Thế Nào?

*(Phần tiếp theo sẽ đi sâu vào kiến trúc MCP, cách triển khai server/client và ví dụ code cụ thể!)*

## Tóm Lại:

- **MCP giúp giảm công sức tích hợp đa nền tảng** → Tiết kiệm thời gian, tập trung vào logic chính.
- **Hỗ trợ cộng đồng rộng lớn** → Dễ dàng mở rộng tính năng.
- **Phù hợp cho AI agent cần tương tác đa nền tảng** (chatbot, automation, data analysis...).