

# MCP & Tool Use

Verbind je agenten met de buitenwereld via het Model Context Protocol

|           |                                |
|-----------|--------------------------------|
| Niveau    | Gevorderd                      |
| Duur      | 4 weken · 3 - 5 uur/week       |
| Lessen    | 9 lessen · ±306 minuten totaal |
| Categorie | Development                    |

## Beschrijving

Het Model Context Protocol (MCP) is dé standaard om agenten met tools en databronnen te verbinden. Leer MCP-servers bouwen en gebruiken, en geef je agenten veilig toegang tot bestanden, databases en API's.

## Voorkennis

- Ervaring met TypeScript of Python
- Basiskennis van AI-agenten en tool use
- Begrip van client-server architectuur

## Wat je leert

- Begrijp het Model Context Protocol: architectuur en filosofie
- Gebruik bestaande MCP-servers in Claude en eigen agenten
- Bouw je eigen MCP-server met tools, resources en prompts
- Ontwerp veilige tool-interfaces met scoping en permissies
- Combineer meerdere MCP-servers in één agent
- Publiceer en versieer je MCP-servers

## Vaardigheden

MCP · Tool design · API's · Security

## Curriculum

### Module 1: MCP-fundamenten

Wat is MCP, waarom is het belangrijk en hoe werkt het onder de motorkap?

#### Wat is MCP en waarom is het een gamechanger? 23 min [video]

Het probleem dat MCP oplost: elke AI-tool heeft zijn eigen integratie. MCP standaardiseert dit.

#### Clients, servers en transports 27 min [video]

De MCP-architectuur: hoe clients en servers communiceren via stdio, SSE en HTTP.

#### Bestaande servers verkennen 30 min [exercise]

Hands-on: verken het MCP-server ecosysteem en koppel een filesystem- en database-server aan Claude.

### Module 2: Zelf MCP-servers bouwen

Bouw je eigen MCP-server met tools, resources en prompts.

#### Je eerste server met de TypeScript SDK 40 min [video]

Stap voor stap een MCP-server bouwen met de officiële TypeScript SDK.

#### Tools, resources en prompts 36 min [video]

De drie MCP-primitieven: tools (acties), resources (data) en prompts (templates).

**Databases en bestanden veilig ontsluiten** 34 min [video]  
Best practices voor het veilig ontsluiten van gevoelige data via MCP.

---

### **Module 3: MCP in productie**

Authenticatie, multi-server architecturen en publicatie.

**Authenticatie en permissies** 28 min [video]  
OAuth, API-keys en permissie-modellen voor MCP-servers in productie.

---

**Multi-server agenten** 33 min [video]  
Combineer meerdere MCP-servers in één agent: filesystem + database + API's.

---

**Eindproject: eigen MCP-ecosysteem** 55 min [project]  
Bouw en publiceer je eigen MCP-server met tools, resources en authenticatie.

---

