Model Context Protocol server/client

HCC AI-Gebruik Interesse groep

Joop Koopman, 11 Oktober 2025

Agenda

- Wat is een AI Agent in algemene zin
- 3 noodzakelijke bouwstenen besproken
- Model Context protocol
- Demo en praktijk

Agents is

1 van de 3 pilaren van AI

Training/Inference/Agents

- Model training = zo veel mogelijk invoer van gegevens
- Inference = Redeneren en conclusies trekken uit data
- Agents
  - Wat is AI-Agent • Een intelligent systeem dat de omgeving observeert, waarneemt
  - Beschikt over intelligentie: analyseren, redenen en kan beslissing nemen
  - Is autonoom, kan acties zelfstandig uitvoeren, zonder tussenkomst van een mens, binnen de gestelde doelen
- uitgebreide presentatie op:

https://ai.hcc.nl/downloads/publieke-downloads/21-node-red-als-agent-7-jun-def-webspdf/file

Motivatie om wat meer van MCP te weten

- Aantal van onze AI agents voorbeelden zijn reeds gebouwd zoals : Verwarming, Nieuws met bezinning quote of the day, Directory opruimen, AI News ophalen en vertalen.

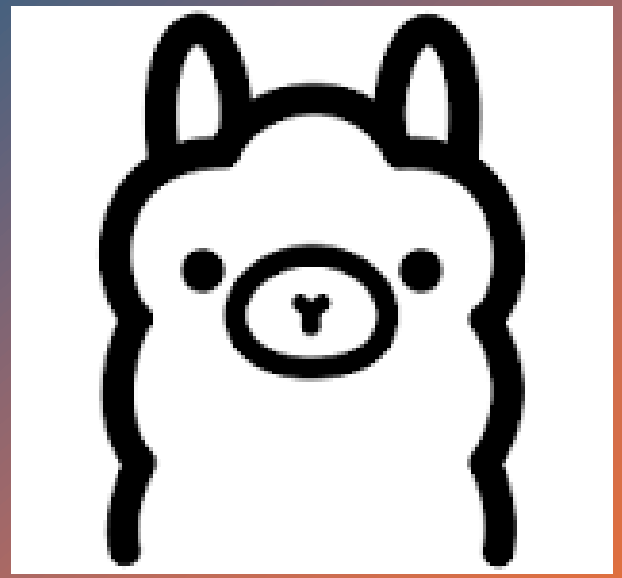
Al deze AI-agents hebben gebruik gemaakt van Node-Red als tool.

MCP voegt een waardevolle standaardisatie toe.

Bouwsteen 1

- Waar hebben we de keus uit ?
  - Grote goede modellen in cloud, of modellen die op je eigen PC te installeren zijn.

- Local LLM = locale Large Language Model voordelen:
  - Gratis (cloud = $$)
  - Privacy gewaarborgd
  - Enorme keuze mogelijkheden.
  - > 1 miljoen modellen, nu, op HuggingFace.
  - **Tools functionaliteit noodzakelijk om met MCP te kunnen werken.**



Bouwsteen 2

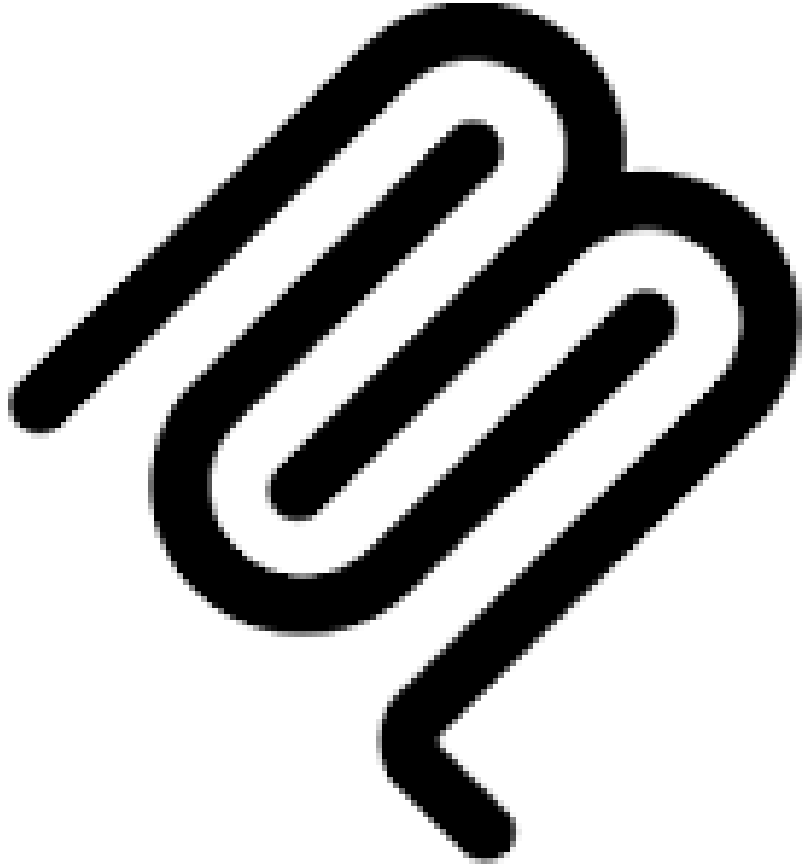
- Keuze uit veel lokale AI programma’s
  - (Jan/GPT4All/LM-Studio/Ollama)
- We kiezen LM-Studio (Windows Only)
- Demo

Bouwsteen 3

- MCP Client/server
  - Tijd
  - E-mail
  - Database
  - Het weer
  - Nieuws berichten
  - Todo
  - etc

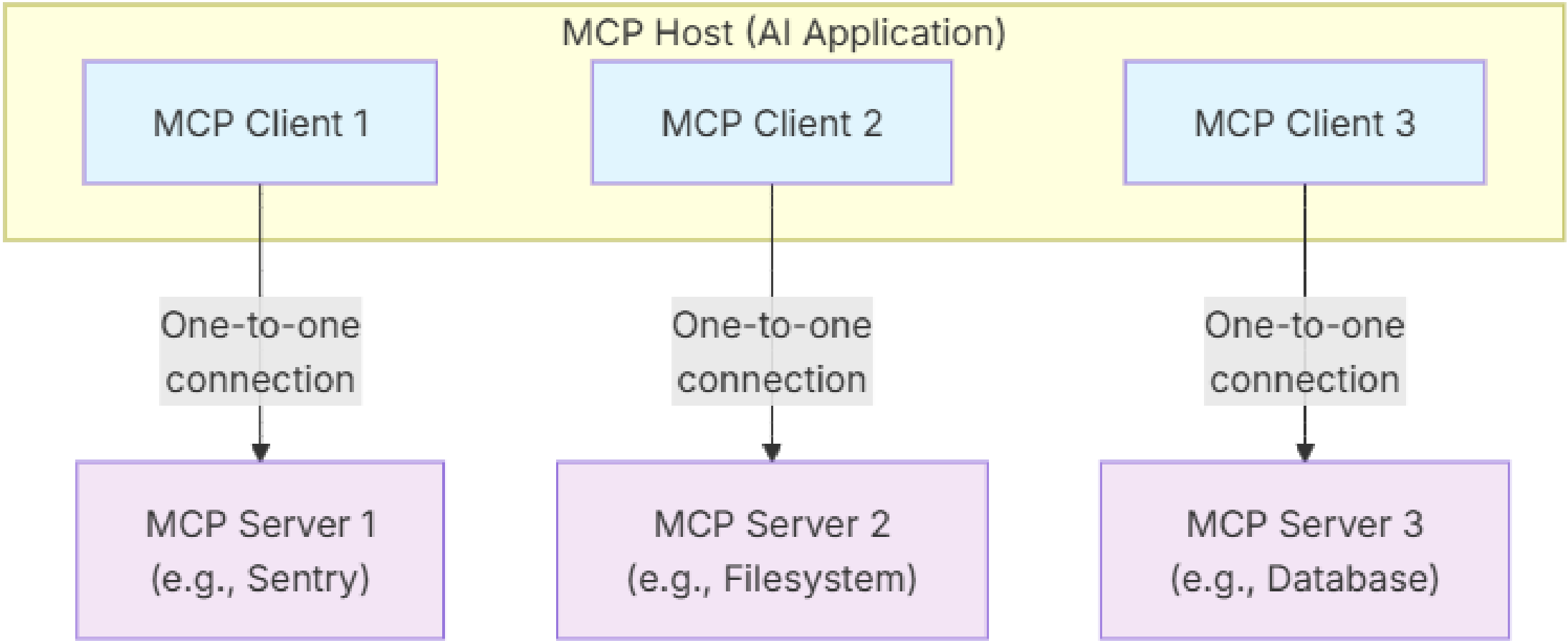
Model Context protocol. Eenvoudig voorbeeld om model slimmer te maken

- **Waarom :**
  - manier om een standaard te formuleren om chaos te voorkomen als iedereen zijn eigen manier ontwikkeld om context te maken
- **Hoe :**
  - Open standaard, dmv een schema geef je aan LLM door welke extra gegevens voor hem beschikbaar zijn. Als gebruiker een vraag stelt aan LLM en LLM besluit dat het antwoord wel eens door een extern programma geleverd zou kunnen worden dan volgt er een communicatie met dat externe programma die het resultaat weer terug geeft aan de LLM. Vervolgens pakt LLM de extra context op en zal dit presenteren.
- **Voorbeeld** LM-Studio zonder time/date MCP integratie en met integratie.



MCP Architecture

- De 3 belangrijke deelnemers in de MCP achitecture zijn :
- **MCP Host**: Het AI programma (bv LM-Studio) dat 1 of meerdere MCP clients coordineert en regelt.
- **MCP Client**: Beheert de verbinding naar de MCP server en ontvangt de context van een MCP server welke gebruikt gaat worden door de MCP Host.
- **MCP Server**: Een programma dat context maakt voor de MCP Clients.


MCP Host (AI Application)
MCP Client 1
MCP Client 2
MCP Client 3
One-to-one connection
One-to-one connection
One-to-one connection
MCP Server 1 (e.g., Sentry)
MCP Server 2 (e.g., Filesystem)
MCP Server 3 (e.g., Database)

Praktisch

- Stappen :
  - Installatie LM-Studio
  - Download model Qwen3:1.7b
  - Voeg “time” mcp functionaliteit toe in LM-Studio
  - Dat is alles, test.

Procedure hoe je “time” MCP server installeert in LM-Studio :

https://lmstudio.ai/blog/lmstudio-v0.3.17

Voorzichtig

- Sommige MCP-servers kunnen willekeurige code uitvoeren, toegang krijgen tot uw lokale bestanden en uw netwerkverbinding gebruiken. Wees altijd voorzichtig bij het installeren en gebruiken van MCP-servers. Als u de bron niet vertrouwt, installeer deze dan niet.

Lijst van beschikbare MCP servers :

https://github.com/modelcontextprotocol/servers?tab=readme-ov-file#-community-servers