

Le Model Context Protocol (MCP)

Standardisation ▪ Connexion Données ▪ Architecture

1. L'IDÉE ESSENTIELLE

Le **Model Context Protocol (MCP)** est un standard ouvert conçu pour connecter de manière sécurisée et universelle les modèles d'intelligence artificielle (LLM) aux sources de données locales ou distantes (fichiers, bases de données, API). Plutôt que de multiplier les connecteurs spécifiques, le MCP offre une **interface standardisée** : un « port USB-C » pour l'IA.

2. ARCHITECTURE ET PRINCIPE DE FONCTIONNEMENT

Le protocole sépare clairement l'application hôte (le client IA) des sources de données (les serveurs MCP) :

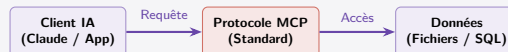
Client MCP (IA) Serveur MCP
(ex: Claude Desktop) Protocol (ex: Base SQL, Fichiers)

— **Clients / Hôtes** : Interfaces d'IA formulant les requêtes. • **Serveurs :Micro** —
programmestransmettantlesrequêtesdel'IAverslesdonnées.

3. EXEMPLE CONCRET : INTERROGER UN DOSSIER LOCAL

1. **Requête** : « Vérifie la configuration de mon site dans mon projet web. »
2. **Médiation** : L'IA interroge le **Serveur MCP** du système de fichiers.
3. **Exécution & Réponse** : Le serveur lit le fichier de façon sécurisée et transmet le contenu au modèle pour correction.

4. FLUX DE COMMUNICATION UNIFIÉ



5. LES BÉNÉFICES DU MCP

- **Sécurité et contrôle** : Maîtrise totale des dossiers et services partagés avec l'IA.
- **Interopérabilité & Modularité** : Un même serveur (ex : GitHub, PostgreSQL) fonctionne avec tout client compatible.

6. Pour aller plus loin : le site officiel MCP

MCP est un sujet assez vaste pour être étudié progressivement. Le projet dispose de son propre site officiel, qui constitue une bonne porte d'entrée pour découvrir son fonctionnement : **Le site officiel** : modelcontextprotocol.io On y trouve notamment :

- une introduction générale, l'architecture **client / serveur** et les rôles (**Hosts, Clients, Servers**) ;
 - les briques exposées : **Tools, Resources et Prompts**, ainsi que des tutoriels pour créer ses propres serveurs.
- À retenir : Passer de la compréhension « qu'est-ce que MCP ? » à « comment fonctionne MCP concrètement ? ».
- Documentation** : <https://modelcontextprotocol.io/>

À RETENIR

« Le MCP résout le problème du cloisonnement des IA en standardisant la manière dont les modèles accèdent aux données externes. »