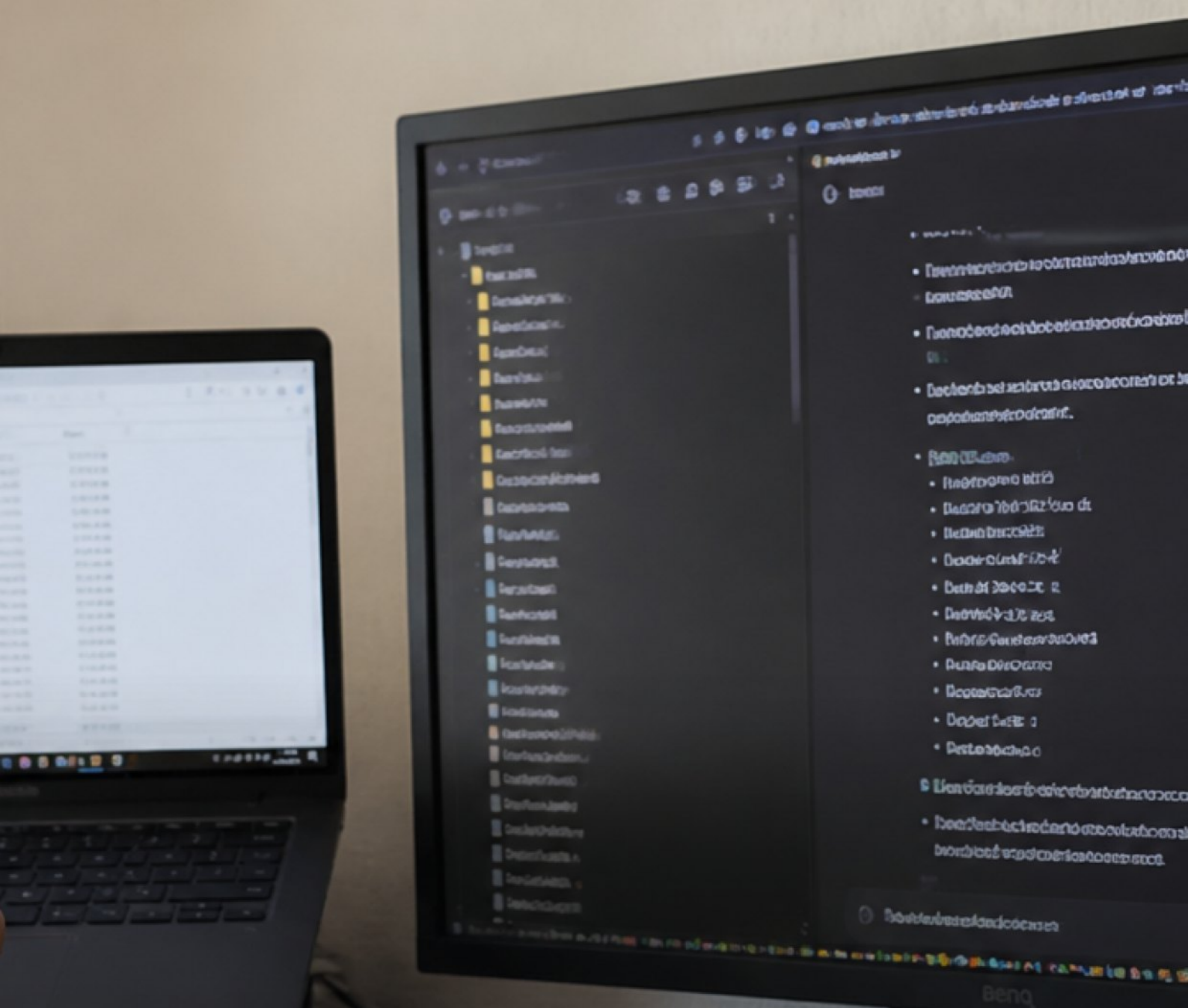




TUTORIEL DE CONNEXION PROGRESSIVE

Brancher un assistant IA à un serveur MCP, sans perdre le contrôle

Utilisez cette feuille de route pour comprendre le rôle de chaque composant, connecter un premier outil de test et vérifier les permissions avant toute action sensible. L'objectif : avancer par petites étapes, avec un périmètre clairement défini.

Au sommaire

- 1 Les repères à garder en tête
- 2 Connecter un premier outil MCP en 6 étapes
- 3 Contrôle avant le premier appel
- 4 Qui fait quoi dans une connexion MCP ?
- 5 En cas de problème, isoler la cause

Les repères à garder en tête

Le serveur MCP expose uniquement les outils, ressources ou fonctions qu'il déclare.

L'assistant interprète la demande, mais ne reçoit pas automatiquement un accès illimité au système.

JSON-RPC 2.0 structure les requêtes et les réponses ; il ne remplace ni l'authentification ni le contrôle des droits.

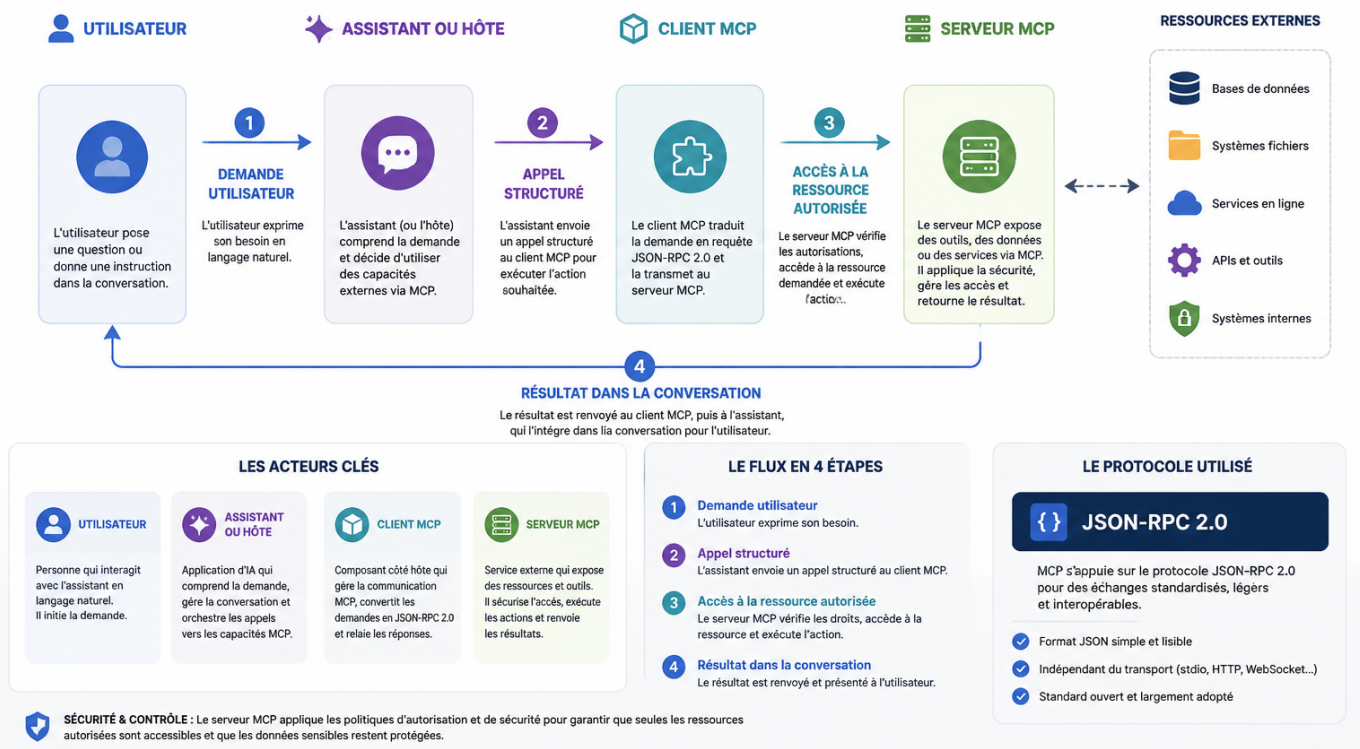
Le client MCP découvre les capacités disponibles, prépare les paramètres et transmet les appels.

La compatibilité dépend de l'assistant, du client, du serveur et du mode de connexion.

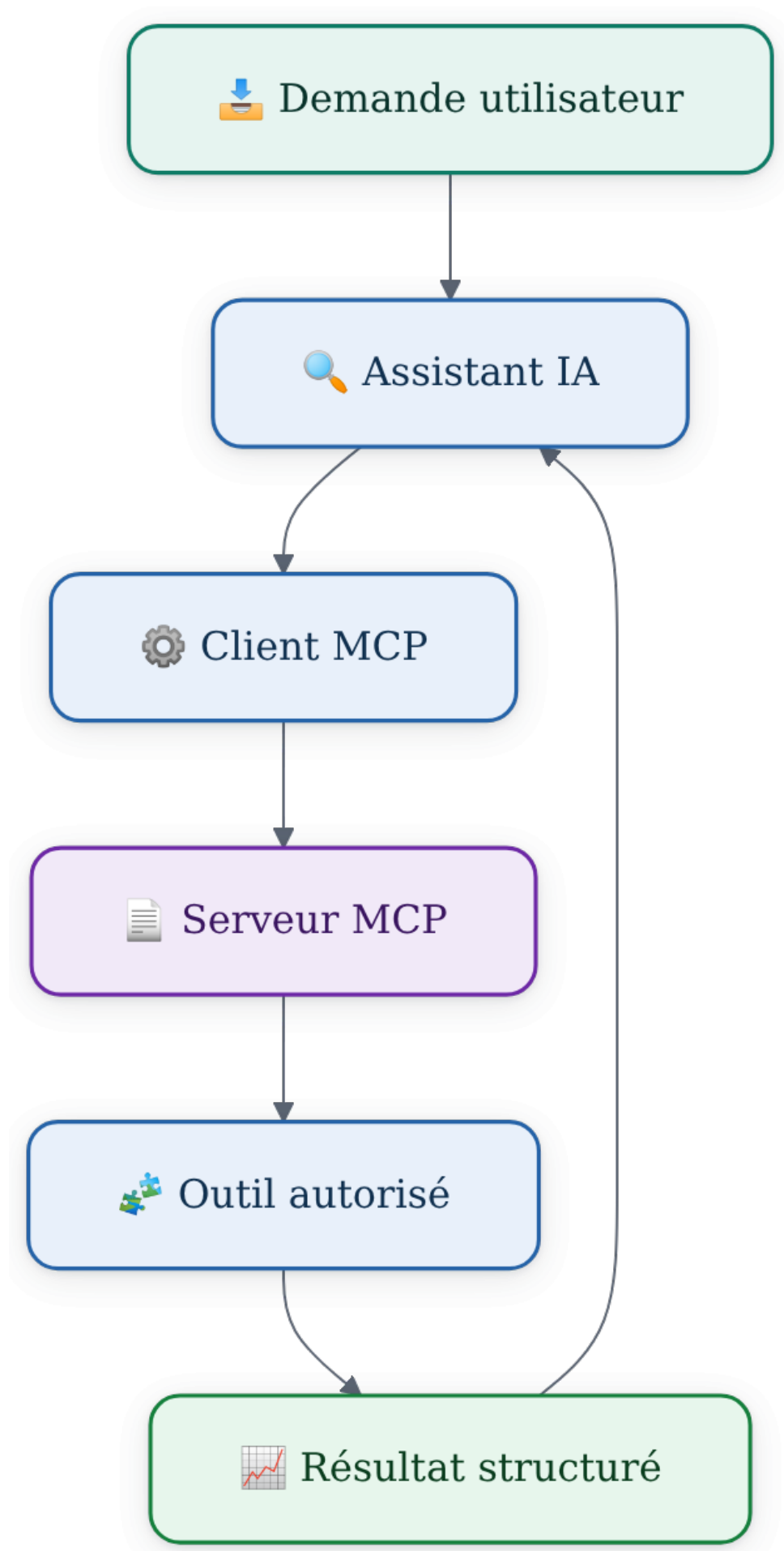
L'ARCHITECTURE D'UN SERVEUR MCP

Un pont sécurisé entre l'IA et vos ressources

Le Model Context Protocol (MCP) standardise la manière dont les applications d'IA accèdent de façon sécurisée aux données et aux outils externes via des serveurs spécialisés.



INFOGRAPHIE Architecture d'un serveur MCP reliant un assistant IA à une ressource autorisée.



Connecter un premier outil MCP en 6 étapes



1. Définir un cas d'usage limité

Choisissez une tâche précise, par exemple rechercher des fichiers dans un dossier de test ou consulter une ressource autorisée. Évitez de commencer par une action de modification, de suppression ou d'envoi.

2. Cartographier les composants

Identifiez l'hôte ou l'assistant, le client MCP, le serveur MCP et la ressource ou l'outil visé. Vérifiez que chacun joue bien son rôle : le serveur expose les capacités, tandis que le client gère la communication.

3. Préparer un environnement de test

Utilisez des données non sensibles et un périmètre isolé. Préparez un dossier ou une ressource dont le contenu est connu afin de pouvoir comparer facilement le résultat attendu et le résultat obtenu.

4. Limiter les capacités exposées

Ne rendez disponibles que les outils et ressources nécessaires au cas d'usage. Commencez par une capacité en lecture seule lorsque cela est possible.

5. Établir la connexion et observer l'appel

Laissez le client découvrir les capacités déclarées, puis vérifiez le nom de l'outil, ses paramètres, la ressource ciblée et la réponse retournée. Une erreur doit être examinée plutôt que contournée.

6. Valider avant d'élargir

Comparez le résultat avec ce qui était attendu. N'ajoutez une nouvelle capacité qu'après avoir confirmé le périmètre, les permissions et le comportement de la première connexion.

Contrôle avant le premier appel

Le cas d'usage est décrit en une phrase

La tâche ne nécessite pas encore de modification, suppression ou envoi.

- Les données de test ne sont pas sensibles**
Le test porte sur une ressource autorisée et contrôlée.
- Le serveur n'expose que les capacités nécessaires**
Les fonctions non utiles au test restent indisponibles.
- Le client MCP et l'assistant sont compatibles avec ce serveur**
La compatibilité n'est pas automatique entre tous les composants.
- Les paramètres attendus par l'outil sont identifiés**
Le client doit transmettre un appel structuré et compréhensible.
- Une validation humaine est prévue pour les actions à impact**
Aucune modification, suppression ou transmission ne doit être exécutée sans confirmation explicite.

Qui fait quoi dans une connexion MCP ?

Composant	Rôle à vérifier
Assistant ou hôte	Interprète la demande et présente le résultat dans la conversation.
Client MCP	Gère la communication, découvre les capacités, prépare les paramètres et transmet les appels.
Serveur MCP	Déclare les outils et ressources, valide les paramètres, vérifie les permissions et exécute les fonctions exposées.
Outil ou ressource externe	Fournit la donnée ou réalise la fonction autorisée par le serveur.

- ! Ne pas confondre découverte et autorisation**
Le fait qu'un outil soit décrit ou découvert ne signifie pas qu'il peut tout faire. Le serveur doit contrôler les paramètres et les permissions. De même, le protocole MCP structure les échanges, mais ne garantit pas à lui seul l'authentification ni la sécurité globale de la connexion.

En cas de problème, isoler la cause

Si la connexion échoue, vérifiez successivement la compatibilité de l'assistant, du client et du serveur, la capacité réellement déclarée, les paramètres transmis, la ressource ciblée et les permissions applicables. Conservez le périmètre de test inchangé pendant le diagnostic afin de distinguer un problème de connexion d'un problème d'autorisation ou d'outil.

À utiliser comme guide de préparation : les modalités exactes de connexion et de permission dépendent de l'assistant, du client MCP, du serveur et de l'environnement utilisés.