Fiche mémo | Leçon 11 | 28 min

Connecteurs, applications, plugins et MCP, comment un agent entre dans vos outils

Un agent entre dans vos outils par un connecteur, nommé à la façon de chaque éditeur : connecteur chez Claude, plugin chez ChatGPT, connecteur Copilot chez Microsoft. Derrière, souvent, le protocole MCP, une prise standard entre agent et logiciel. Vous apprenez à brancher un connecteur, à en ajouter un par son adresse et à le débrancher.

Objectifs

- Expliquer à un collègue, sans jargon, ce que font un connecteur, un serveur MCP et une connexion OAuth
- Brancher un connecteur de l'annuaire, puis un connecteur personnalisé par l'adresse de son serveur
- Inventorier les outils d'un connecteur, distinguer lecture et écriture, et révoquer un accès au bon endroit

À retenir

- Connecteur chez Claude, plugin chez ChatGPT, connecteur Copilot chez Microsoft : le même principe, un agent branché sur un logiciel.
- MCP est une prise standard : l'agent liste les outils du serveur, choisit d'après leur description, appelle, lit la réponse.
- « Se connecter avec » passe par la page de l'éditeur : l'agent reçoit un jeton limité à vos droits, jamais votre mot de passe.
- Un connecteur personnalisé n'est pas vérifié par Anthropic : seulement un serveur d'organisation de confiance, inventorié avant usage.
- L'accès se coupe là où il a été branché, dans l'agent ; débranchez ce qui ne sert plus.

La demande à recopier

Demande à recopier **Fiche MANDAT pour inventorier un connecteur avant de s'en servir**

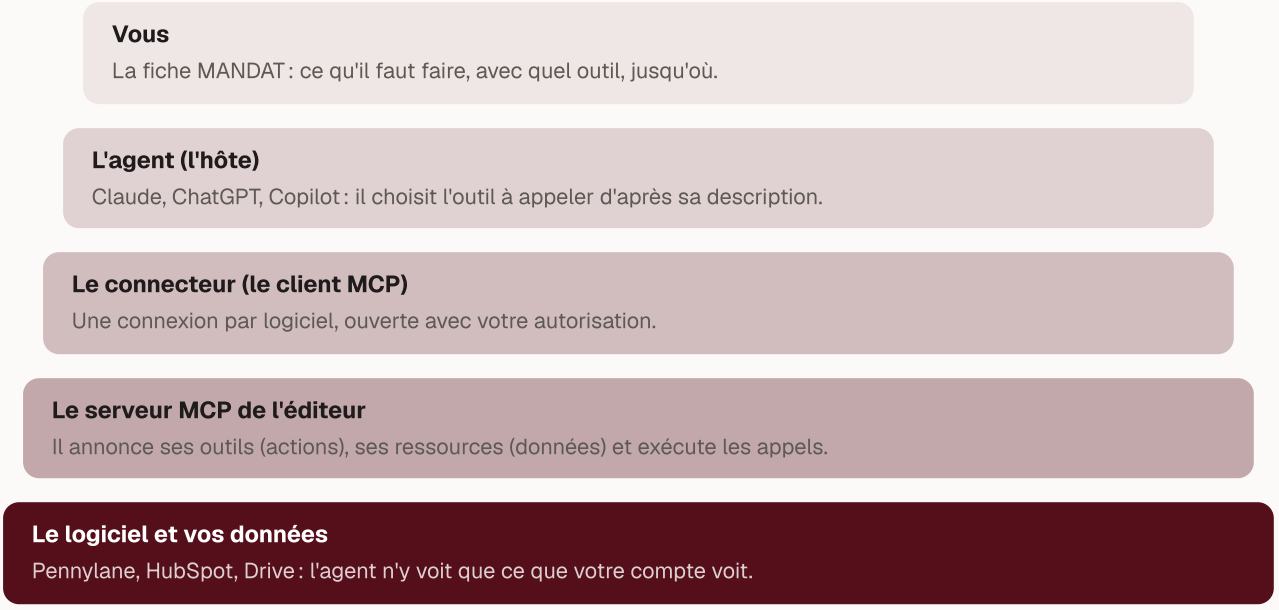
```
MISSION : un tableau des outils que le connecteur [nom du connecteur] met à ta disposition.
APPUIS : la liste des outils et leurs descriptions, telles que le connecteur te les annonce.
NIVEAU D'ACCÈS : aucun appel d'outil ; aucune donnée du logiciel lue.
DÉROULÉ : 1. Une ligne par outil : nom, ce qu'il fait d'après sa description, paramètres
attendus. 2. Classe chaque outil : lecture, brouillon, modification ou création, envoi ou
partage, suppression ou paiement. 3. Si la description est trop vague pour classer, écris [À
CLARIFIER].
ARRÊTS : n'appelle aucun outil, même pour tester. Ne lis aucune donnée.
TERMINÉ QUAND : chaque outil annoncé figure dans le tableau avec une classe ou [À CLARIFIER] ;
tu rends le nombre d'outils par classe.
```

Note : Ce tableau sert à régler les droits outil par outil, et à refuser un connecteur qui écrit davantage que la tâche ne l'exige.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Coller un identifiant et un mot de passe dans la conversation pour que l'agent « se connecte ». Le secret reste dans l'historique, se retrouve dans les partages de conversation, et donne à l'agent tous vos droits sans jeton révocable.	Passez par un connecteur dont la connexion s'ouvre sur la page de l'éditeur ; s'il n'en existe pas, la tâche attend.
Ajouter un connecteur personnalisé trouvé sur un forum ou envoyé par un inconnu. Il n'est pas vérifié, ses outils peuvent écrire ou exporter, et vos données transitent par un serveur dont vous ne savez rien.	Ne branchez que le serveur officiel de l'éditeur du logiciel ou d'un prestataire sous contrat, et faites inventorier ses outils avant tout usage.
Laisser tous les connecteurs actifs dans toutes les conversations. L'agent peut appeler un outil d'un logiciel qui n'a rien à voir avec la tâche, et une consigne piégée trouve plus de portes ouvertes.	Activez par le bouton + seulement les connecteurs de la tâche, dans la conversation de la tâche.
Croire qu'un départ de salarié coupe l'accès de son agent dès que son compte du logiciel est fermé. Pour certains logiciels, comme Pennylane, la révocation de l'assistant se fait côté assistant. Un connecteur oublié reste une porte, au moins jusqu'à la fermeture effective du compte.	Dans la procédure de départ, supprimez le connecteur dans l'agent, retirez le compte de l'organisation de l'agent et fermez l'accès au logiciel.

Du clic à l'action dans le logiciel



Le protocole MCP relie l'agent au logiciel ; vos droits dans le logiciel restent la limite.