Corrigé

P1C5 - Comprenez comment connecter l'IA à vos outils avec le protocole MCP

Note de cadrage : connecter un assistant IA aux outils Storra via MCP

Destinataires : équipe dirigeante StorraRédigée par : chef de projet no-code

1. Quels outils et données exposer à l'assistant IA, et pourquoi ?

Deux ressources sont prioritaires pour une première expérimentation à faible risque.

- Le catalogue produits (Airtable) : c'est une donnée stable, non sensible, et fréquemment interrogée par les clients. Exposer ce catalogue à un assistant IA lui permettrait de répondre aux questions produits en temps réel, sans intervention humaine.
- L'historique des commandes (via l'API Storra) : c'est une donnée opérationnelle clé. Un assistant IA qui y a accès peut détecter des anomalies, identifier des commandes bloquées, et alerter l'équipe avant qu'un client ne se manifeste.

Les données clients (HubSpot) ne sont pas recommandées pour une première phase : elles sont plus sensibles et nécessitent un niveau de gouvernance plus élevé.

2. Quelles actions concrètes l'assistant IA pourrait-il réaliser ?

Avec un accès au catalogue produits via MCP, l'assistant IA pourrait : répondre automatiquement aux questions de disponibilité produit, suggérer des alternatives si un article est en rupture, et mettre à jour une fiche produit sur instruction en langage naturel.

Avec un accès à l'historique des commandes, il pourrait : générer un rapport quotidien des commandes en attente, détecter les commandes bloquées depuis plus de 48 heures, et déclencher une alerte vers l'équipe logistique.

3. Quels garde-fous mettre en place ?

Trois règles non négociables avant toute mise en production.

- *Périmètre d'action délimité :* l'assistant IA n'a accès qu'aux ressources explicitement exposées via MCP. Il ne peut pas accéder aux données clients, aux informations financières, ni à aucun outil non listé dans la configuration MCP.
- *Supervision humaine systématique :* dans un premier temps, toute action déclenchée par l'IA doit être validée par un membre de l'équipe avant exécution. L'IA propose, l'humain décide.
- *Traçabilité des actions :* chaque action réalisée par l'assistant via MCP est enregistrée dans un journal d'audit, consultable à tout moment. En cas d'erreur, vous pouvez identifier exactement ce qui s'est passé et sur quelles données.

MCP est une technologie prometteuse, mais encore jeune. L'approche recommandée est de démarrer sur un périmètre restreint, mesurer les résultats, et étendre progressivement — exactement comme vous l'avez fait avec les automatisations no-code depuis le début de ce projet.