Fiche mémo · Leçon 22 · 26 min

# Ce qu'un agent IA change dans un flux, et quand vous en passer

Un agent IA ne suit pas un chemin écrit d'avance : il reçoit un objectif et des outils, et choisit lui-même, appel après appel, quoi faire jusqu'au résultat. Il sert quand les demandes varient trop pour des règles. Ailleurs, un flux avec une étape IA fait le même travail, moins cher, plus prévisible et plus facile à contrôler.

## Objectifs

- Distinguer un flux avec une étape IA d'un agent qui choisit lui-même ses outils
- Décider avec quatre questions si une tâche justifie un agent
- Estimer le coût et les risques d'un agent avant de le construire

## À retenir

- Un agent choisit lui-même ses outils, tour après tour ; un flux suit le chemin que vous avez écrit.
- La plupart des tâches d'une PME se font mieux avec un flux et une étape IA : moins cher, plus prévisible.
- Un agent se justifie quand les demandes varient trop et qu'il faut chercher à plusieurs endroits selon le cas.
- Le modèle ne connaît vos outils que par leur description : elle doit dire ce qu'ils font, attendent et rendent.
- Outils en lecture seule d'abord, validation humaine sur tout ce qui agit, limite de tours et de budget.

## La boucle d'un agent

**1 — Lire l'objectif**

La demande, la consigne système et ce que la mémoire a gardé.

**2 — Choisir un outil**

Le modèle lit la description des outils et décide lequel appeler, avec quels paramètres.

**3 — Agir**

L'outil s'exécute : lecture d'un tableur, recherche, brouillon, appel d'un service.

**4 — Observer**

Le résultat revient au modèle, qui recommence ou rédige sa réponse.

Chaque tour est un appel au modèle, donc des jetons. La boucle s'arrête sur une réponse ou sur une limite.

## La demande à recopier

**Demande à recopier** Faire examiner une idée d'agent avant de la construire

```
Tu es consultant en automatisation pour des PME. Voici une tâche que nous voulons confier à un agent IA : [décrivez la tâche, le volume par mois, les logiciels concernés et les données traitées].
Réponds aux quatre questions suivantes, chacune en deux lignes : 1. Les demandes varient-elles au point qu'aucun enchaînement fixe ne couvre la plupart des cas ? 2. Faut-il plusieurs outils dans un ordre qui dépend du cas ? 3. Chaque action qui sort de l'entreprise peut-elle être validée par une personne ? 4. Le gain couvre-t-il plusieurs appels au modèle par demande ?
Puis : si un flux avec une étape IA suffit, décris-le en cinq étapes. Si un agent se justifie, liste ses outils, en marquant chacun « lecture seule » ou « agit », et dis lesquels doivent être validés par une personne.
```

## Le code à recopier

**Trois descriptions d'outils bien écrites** TEXT

```
chercher_commande
  Cherche une commande dans le tableur des commandes, par numéro (format 2026-1234)
  ou par adresse électronique du client. Lecture seule : ne modifie rien.
  Rend : numéro, statut, date d'expédition, transporteur, numéro de suivi.
  À employer avant toute réponse sur une livraison.

lire_conditions_retour
  Rend le texte des conditions de retour et de garantie en vigueur.
  Lecture seule. À employer pour toute question de retour, d'échange ou de garantie.

creer_brouillon
  Crée un brouillon de réponse dans la boîte sav@, sans l'envoyer.
  Paramètres : destinataire, objet, corps. Une personne relit et envoie.
```

Aucun outil « envoyer » ni « supprimer » : l'agent prépare, une personne décide. C'est le premier garde-fou.

## Les erreurs fréquentes

| L'erreur, et pourquoi elle coûte | La correction |
|---|---|
| **Construire un agent pour une tâche dont les règles s'écrivent, parce que le mot est à la mode.** L'agent appelle le modèle plusieurs fois, suit un chemin différent à chaque demande et se teste mal ; un flux ferait mieux pour moins cher. | Passer la tâche aux quatre questions et s'arrêter au premier « non » : le plus souvent, une étape IA dans un flux suffit. |
| **Donner à l'agent un outil qui envoie, paie ou supprime, sans validation humaine.** Un courriel lu par l'agent peut contenir des instructions qui le détournent ; une action partie ne se rattrape pas. | Outils en lecture seule, brouillon à la place de l'envoi, validation humaine sur chaque outil qui agit, aucun outil de suppression. |
| **Écrire des descriptions d'outils d'un mot (« commandes », « clients »).** Le modèle ne voit que ces descriptions : il appelle l'outil au hasard, recommence, et chaque tour coûte. | Pour chaque outil, dire ce qu'il fait, ce qu'il attend, ce qu'il rend et quand l'employer, comme dans le modèle de la leçon. |
| **Retirer la limite de tours ou de tâches « pour que l'agent aille au bout ».** Un agent qui ne trouve pas peut boucler longtemps ; la facture de jetons ou de tâches suit. | Garder une limite basse (5 à 10 tours dans n8n, 75 tâches chez Zapier) et lire les exécutions qui l'atteignent. |