

Agents IA et MCP : garder le contrôle

Mémo d'atelier · SDK Python 2.2.0 · 30 septembre 2026

1. Les trois rôles

- Modèle : propose une réponse ou un appel.
- Agent : organise la boucle, son budget et son arrêt.
- MCP : protocole d'échange ; ne définit pas tes permissions.

2. Laboratoire

- VM serveur, compte ordinaire, Python 3.10+, environnement virtuel.
- Installer mcp==2.2.0 et conserver pip freeze.
- Client(mcp) : test en mémoire, aucun port public.

3. Outil minimal

- Une fonction de lecture ; deux identifiants autorisés.
- Aucun shell, URL arbitraire ou chemin libre.
- Liste d'outils autorisés et contrôle des arguments avant l'appel.

4. Données et permissions

- Une instruction dans un document reste une donnée extérieure.
- Limiter lectures, durée, volume et nombre d'étapes.
- Les droits du compte système doivent correspondre au besoin réel.

5. Avant toute mutation

- Préparer un brouillon séparément de la publication.
- Afficher contenu, destination et modifications exactes.
- Approbation liée à cette version ; vérifier identité et droits côté serveur.

6. Contrôles et arrêt

- Fiche RAW : résultat attendu égal au texte du catalogue.
- Outil inconnu : refus avant appel ; injection : aucune publication possible.
- Journaliser les refus sans recopier les secrets ; arrêter sur erreur.
- Finir avec deactivate ; aucun timer créé par cet atelier.

Article complet, exercices et sources : blog.gringao.fr/ia-agents-mcp-outils-permissions/