

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/

Vidéo -> sous-titres -> brouillon

Mémo d'atelier · faster-whisper 1.2.1 · sur serveur

1. Préparer

- Ton média, un extrait de 2 à 5 minutes, une copie de travail.
- Compte ordinaire et environnement Python sur serveur.
- Conserver l'original, les versions et les sorties distinctes.

2. Audio

- Vérifier les pistes avec ffprobe.
- Extraire la bonne piste en mono PCM 16 bits, 16 kHz.
- Écouter début, passages faibles et fin ; ne pas écraser la source.

3. Transcription

- Point de départ : small multilingue, CPU INT8, langue fr, VAD.
- Consommer les segments du générateur.
- Conserver id, début, fin et texte dans le JSON.
- SRT : HH:MM:SS,mmm ; lignes numérotées et séparées par une ligne vide.

4. Relecture

- Noms propres, chiffres, négations, termes techniques.
- Écouter les passages silencieux et les segments incertains.
- Découper naturellement les longues phrases ; ajuster la durée à l'audio.
- Conserver [S001], etc., dans la transcription corrigée.

5. Brouillon IA

- Utiliser la transcription validée, sur une interface serveur locale vérifiée.
- Chaque fait doit renvoyer à des segments existants.
- Information absente : signaler le manque, ne pas compléter.
- Fournir titre réel, date et lien d'origine séparément.

6. Validation et suite

- Comparer une minute témoin à une transcription manuelle.
- Rejeter toute donnée inventée, même plausible.
- Publier seulement après contrôle éditorial.
- Future routine : serveur, anti-doublons, état des traitements, brouillons.

Article complet, exercices et sources : blog.gringao.fr/ia-video-transcription-sous-titres-article/

PDF et IA : extraire sans inventer

Mémo d'atelier · OCR, JSON et contrôle des preuves

1. Identifier le PDF

- Texte sélectionnable : essayer l'extraction directe.
- Scan : OCR ; document mixte : --skip-text.
- Une couche OCR mauvaise demande un autre diagnostic ; conserver l'original.

2. Préparer l'OCR

- VM serveur isolée pour les fichiers non fiables.
- Tesseract fra+eng ; vérifier les langues installées.
- Document net, plat, éclairage uniforme ; scan proche de 300 dpi.
- Contrôler visuellement rotation et redressement.

3. Préserver la provenance

- Empreinte du fichier, nom de source, page et versions des outils.
- Un fichier texte par page pour le premier pipeline.
- Pour chaque champ : valeur brute, page, extrait exact.

4. Extraire

- Ollama local au serveur, adresse 127.0.0.1:11434.
- Schéma explicite ; réponse contrôlée avec Pydantic.
- Valeur absente : valeur, page et extrait = null.
- Interdire les champs inattendus et conserver les erreurs.

5. Trois niveaux de contrôle

- Structure : clés et types conformes.
- Provenance : extrait présent dans la page, contenant la valeur.
- Sens : total TTC et date de facture, pas un montant ou une date voisins.
- Lire l'original : OCR, signes, virgules, devise et caractères O/O.

6. Évaluer et revenir en arrière

- Facture fictive témoin ; retirer un champ pour tester null.
- Comparer dix documents à des réponses préparées à la main.
- Valeurs contradictoires entre pages : revue humaine.
- Garder originaux, travail et sorties séparés ; aucun import métier automatique.

Article complet, exercices et sources : blog.gringao.fr/ia-documents-pdf-ocr-json-fiable/

Comptes : protection et secours

Passkeys, MFA et récupération · Mémo à conserver sans y inscrire de secrets

Comparer

- Mot de passe : unique, long, généré par un gestionnaire.
- TOTP : code temporaire ; la graine et son QR code restent secrets.
- Passkey : authentification liée au service, résistante au phishing de connexion.

Choisir

- Identifie le fournisseur qui stocke/synchronise la passkey.
- Distingue synchronisation et authenticateur lié à un appareil.
- Une clé USB OTP n'est pas automatiquement une clé FIDO2.

Préparer le secours

- Vérifie et protège l'email de récupération.
- Enregistre un second moyen, si le service le permet, et range-le séparément.
- Garde les codes de récupération dans un stockage protégé accessible sans le téléphone.

Tester sans se bloquer

- Commence sur un compte test, sans effacer de téléphone ni retirer le dernier accès.
- Essaie la connexion principale dans un autre profil de navigateur.
- Simule la perte : n'utilise pas le téléphone et essaie le secours.

Résultat attendu

- L'accès de secours fonctionne sans le moyen déclaré perdu.
- Les dépendances et les notifications de sécurité sont comprises.
- Marque les codes consommés ; renouvelle et range le lot si nécessaire.

Entretenir

- Note service, moyens, emplacement des secours et date du dernier essai.
- Refais le test après changement d'appareil ou de fournisseur.
- Une passkey ne protège pas toutes les sessions ni tous les parcours de récupération.

Article complet, exercices et sources : blog.gringao.fr/cyber-passkeys-double-authentication-recuperation/

WordPress : sécurité sans régression

Formulaires, visiteurs et moteurs · Un changement à la fois

Observer

- Identifie chaque formulaire et son endpoint : contact, livre d'or et commentaires peuvent différer.
- Corrèle un spam avec date, module et journal ; masque les données personnelles.
- Note l'état initial : versions, protections, acceptations et refus.

Préparer

- Sauvegarde fichiers + base et prépare une restauration testée.
- Préproduction privée ; emails capturés ou bloqués.
- Écris réglage, résultat attendu, test et retour arrière.

Traiter côté serveur

- Validation avant stockage/envoi ; les vérifications JavaScript sont contournables.
- Honeypot réellement vérifié ; test avec autofill et clavier.
- Défi anti-bot : refus si preuve absente/expirée ; compatibilité avec le cache.

Limiter avec mesure

- Sépare envoi du formulaire, connexion et lecture des pages.
- Déduis les seuils du trafic ; une IP peut représenter un réseau partagé.
- Message de refus utile, délai connu et retour à la normale testé.

Préserver le référencement

- Vérifie HTTP, robots.txt, balise robots, X-Robots-Tag, canonique et sitemap.
- Un User-Agent Googlebot ne prouve pas l'identité du robot.
- Un accès réussi ou une indexation demandée ne garantit pas l'indexation.

Six tests

- Message normal : confirmation et une seule réception.
- Champ requis absent / adresse invalide : aucun email.
- Honeypot ou preuve anti-bot invalide : refus serveur.
- Rafale contrôlée puis attente : limite et récupération observées.
- Article + rubrique + sitemap : lisibles sans défi inattendu.

Article complet, exercices et sources : blog.gringao.fr/cyber-wordpress-securiser-formulaires-referencement/

WordPress : prouver sa restauration

Laboratoire sur serveur · Chemins et identifiants distincts de la production

Définir

- RPO : durée de données perdues acceptable. RTO : durée visée de retour du service.
- Prépare des témoins : article, média, PDF, rubrique et compte test.
- Chronomètre depuis la recherche de l'archive jusqu'aux vérifications finales.

Sauvegarder

- Lot = base + fichiers + versions + informations d'exploitation.
- Répertoire privé hors HTTP ; chiffrement et clé récupérable séparément.
- Assure la cohérence base/fichiers ; transaction SQL seule ≠ snapshot global.
- Copies séparées, générations protégées et empreintes de référence fiables.

Isoler avant démarrage

- VM serveur dédiée sans route vers Internet ni production, y compris IPv6.
- Pas de volume prod, compte DB prod, clé SSH prod ni socket Docker.
- Teste le filtrage avec des cibles témoins autorisées ; vérifie ses journaux.

Neutraliser la copie

- Configuration et secrets de laboratoire ; tâches serveur et cron vérifiés.
- MU-plugin : bloque wp_mail et l'API HTTP WordPress.
- Ces filtres ne bloquent pas SMTP/cURL directs : garde l'isolation réseau.
- Client navigateur isolé, pour éviter les requêtes vers des médias externes.

Restaurer

- Vérifie empreintes, chemins et liens avant extraction dans une arborescence neuve.
- Avant db import : contrôle DB_HOST, DB_NAME et chemin /srv/lab/wp.
- search-replace : dry-run, périmètre de tables défini, données sérialisées préservées.
- Applique uniquement au labo après lecture du rapport ; pas de DNS public modifié.

Prouver et améliorer

- Contenus, médias, liens, connexion et fonctions utiles vérifiés.
- Aucun mail réel ni appel externe ; collecteur de test uniquement interne.
- Mesure perte constatée et temps total, compare aux RPO/RTO.
- Corrige puis refais le test ; l'existence d'une archive ne prouve pas la récupération.

Article complet, exercices et sources : blog.gringao.fr/cyber-sauvegarde-restauration-wordpress-isolee/

Mémo RAW · darktable 5.6

Du négatif numérique au JPEG cohérent, sans perdre les sources

Avant import

- Copier la carte, compter et contrôler quelques fichiers.
- Faire une seconde copie sur un autre support.
- Conserver RAW et futurs XMP ensemble ; ne pas écraser les originaux.

Tri

- Rejeter flou/moment raté, comparer les quasi-doublons.
- Définir une convention étoiles/étiquettes stable.
- Choisir une image témoin par lumière comparable.

Développement

- Contrôler écrêtage RAW et zones importantes.
- Exposition : placer les tons moyens.
- Une seule transformation d'affichage : sigmoid, filmic rgb ou AgX.
- Correction couleur crédible avant style créatif.

Détails

- Réduire le bruit à 100 %, puis juger à taille de sortie.
- Masques locaux seulement si un problème reste local.
- Comparer visage, cheveux, tissu, ombres et hautes lumières.

Export web

- JPEG avec profil sRGB et dimensions adaptées.
- Vérifier les métadonnées de localisation/crédit.
- Ouvrir le JPEG hors de darktable ; comparer couleur et netteté.

Dépannage

- Rendu différent : vérifier profils écran et export.
- Réglages absents : chercher RAW, XMP et chemins du catalogue.
- Ombres très bruitées : revenir au RAW ; ne pas inventer du détail.

Article complet, exercices et sources : blog.gringao.fr/photo-developper-raw-darktable/

Mémo flash · TTL et manuel

Réglage de départ, direction de lumière et diagnostic sur place

Compatibilité

- Vérifier boîtier + flash + déclencheur : TTL, HSS, radio et obturateur.
- Repérer la synchro X du boîtier ; prendre une marge avec radio.
- Tester batterie, groupe, canal et recyclage.

Choisir le contrôle

- TTL : distance ou sujet variable ; correction flash si estimation décalée.
- Manuel : géométrie stable, puissance constante.
- Mode M du boîtier compatible avec TTL du flash.

Plan 1 · rebond

- Surface blanche proche, renvoyer la lumière vers le visage.
- Vue sans flash, puis TTL à correction zéro.
- Si plafond haut/coloré : changer de surface.

Plan 2 · déport

- Source vers 45° et légèrement au-dessus ; support stable.
- Commencer à faible puissance, faire une vue témoin.
- Ombre dure : rapprocher/agrandir la source.

Plan 3 · contre-jour

- Exposer d'abord le fond ; flash de remplissage modéré.
- Au-delà de X : HSS seulement si compatible ; portée réduite.
- Alternative : filtre ND, source plus proche, retour sous X.

Erreurs rapides

- Bande noire : vitesse/synchro/latence radio.
- Flash absent : obturateur électronique ou mode silencieux ?
- Sujet « fantôme » : pose ambiante trop longue.
- Sujet trop clair : correction TTL ou puissance manuelle, pas seulement vitesse.

Article complet, exercices et sources : blog.gringao.fr/photo-flash-ttl-manuel-deporte/

Mémo concert · soirée · nuit

Préparer la série, contrôler le scintillement, raconter la soirée

Avant

- Accès, placement et règles de flash validés auprès de l'organisateur.
- Batteries/cartes prêtes ; RAW ; trois positions repérées.
- Prévoir large, visage, détail, relation, public, fin.

Exposition

- Regarder visage et hautes lumières, pas la moyenne de la salle noire.
- Départ conditionnel : ~1/250 s calme, ~1/500 s geste rapide ; vérifier à 100 %.
- ISO nécessaire selon ton boîtier ; ne pas sous-exposer par principe.

Mise au point

- AF œil/visage si fiable, petite zone si micro/fumée/contre-jour trompent.
- Rafales courtes au moment du geste.
- Photo témoin agrandie sur l'œil ou le détail voulu.

Couleur

- RAW et balance auto si éclairages changeants ; valeur fixe si stables.
- Garder les couleurs voulues de scène, sans neutraliser tous les gels.
- Traiter les images par groupes de lumière comparable.

Bandes

- 50 Hz secteur : parfois 100 Hz ; LED PWM parfois bien plus rapide.
- Tester plusieurs vitesses et mécanique/électronique sur photo enregistrée.
- Anti-scintillement 100/120 Hz ou vitesse variable selon modèle ; pas de valeur universelle.

Sélection

- Six images utiles plutôt que six doublons.
- Écarter bandes et flous non voulus ; légendes vérifiées.
- Couverture lisible en miniature, lien vers album complet.

Article complet, exercices et sources : blog.gringao.fr/photo-concert-soiree-nuit/