Formation Mise en place d’un Model Context Protocol (MCP)

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : MMCP

Niveau : Facile

intra

Mise à jour le 22/09/25

*tarif valable jusqu'au 31/12/2025

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Bonne maîtrise de Python et des bases du développement logiciel (gestion de packages, environnements virtuels, APIs)
- Connaissances en architectures IA / LLMs (utilisation de modèles, intégration d’APIs, gestion de contextes)
- Notions en systèmes distribués et sécurité (protocoles client-serveur, authentification, échanges sécurisés)

Objectifs

Objectifs pédagogiques :

- Comprendre le rôle du MCP
- Découvrir les standards de métadonnées et contextes
- Apprendre à créer un prototype MCP

Objectifs opérationnels :

- Concevoir, déployer et intégrer le Model Context Protocol dans une architecture IA : installer et configurer des serveurs et clients MCP, exposer des ressources et outils externes, sécuriser les échanges de contexte partagé, et rendre ses agents ou applications LLM capables d’interagir dynamiquement avec des systèmes externes selon le protocole standard.

Programme

Jour 1 – Introduction au MCP

Introduction et contexte
Présentation générale du Model Context Protocol (MCP) et de sa finalité
Historique et évolution des standards de communication pour agents IA
Enjeux liés à l’interopérabilité des modèles d’IA, des workflows et des systèmes externes
Cas d’usage : intégration avec bases de données, APIs, applications métiers et LLMs
Architecture et composants
Structure générale d’un MCP : serveurs, clients, ressources et contextes
Définition des ressources exposées et des flux de données
Communication client-serveur : protocole, messages et formats standard
Sécurité et contrôle d’accès : authentification, autorisations, confidentialité des données
Comparaison avec d’autres standards ou méthodes d’interaction IA
Standards et bonnes pratiques
Modélisation des contextes pour agents IA
Normes ouvertes et compatibilité avec LLMs et outils existants
Stratégies pour la modularité, la scalabilité et la maintenabilité
Études de cas illustratives : mise en œuvre de MCP dans différents secteurs (finance, e-commerce, santé)

Jour 2 – Atelier pratique

Création d’un MCP
Installation et configuration des serveurs MCP
Développement d’un client MCP pour exposer des ressources et récupérer des contextes
Définition et modélisation des contextes : structuration des données, types de ressources et relations
Intégration avec un LLM ou un agent IA simple pour exploiter le contexte
Déploiement et démonstration
Lancement du MCP dans un environnement de test

Test des échanges client-serveur et vérification des accès aux ressources
Déploiement sur un cas concret : interfaçage avec une base de données, un fichier ou une API
Démonstration complète : un agent IA accède à un contexte externe et effectue une tâche (extraction d’information, interaction avec des outils métiers)
Analyse des logs, suivi des interactions et identification des optimisations possibles

Conclusion et bonnes pratiques

Revue des points clés et checklist pour la mise en production
Bonnes pratiques pour la sécurité, la scalabilité et la maintenabilité des MCP