

Mis à jour le 13/10/2026

S'inscrire

Formation Certification MCP fondamentaux : mise en pratique

3 jours (21 heures)

Présentation

Donnez à vos applications agentiques un accès maîtrisé aux outils et aux données de votre entreprise. Avec le Model Context Protocol et une approche centrée sur les clients, serveurs et transports, apprenez à concevoir des intégrations interoperables, sécurisées et adaptées aux contraintes de production.

Notre Formation Certification MCP fondamentaux : mise en pratique vous prépare à la certification officielle MCPA en associant compréhension du protocole, exercices guidés et analyse de situations représentatives des compétences évaluées à l'examen.

Vous apprendrez à développer un client MCP, à construire un serveur exposant des outils et des ressources, puis à connecter des API externes à un workflow utilisant un modèle de langage.

À l'issue de la formation, vous serez en mesure de gérer les requêtes sans état, de contrôler les autorisations, de limiter les risques liés aux outils et de diagnostiquer les erreurs d'intégration.

Le parcours aborde également les tests et l'observabilité, les choix d'architecture et la gouvernance des catalogues. Des ateliers progressifs et une évaluation blanche vous aideront à consolider votre préparation à l'examen et à transposer ces acquis dans vos projets.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Expliquer les rôles des hôtes, clients et serveurs dans une architecture MCP et distinguer outils, ressources et prompts
- Développer un client MCP intégré à un workflow utilisant un modèle de langage
- Construire un serveur MCP exposant des outils, des ressources et des API externes
- Mettre en œuvre des interactions sans état avec métadonnées par requête et état applicatif explicite
- Sécuriser et tester les intégrations avec des contrôles d'accès, des validations et des traces d'audit
- Préparer l'examen MCPA par l'analyse de scénarios et une évaluation blanche

Public visé

- Développeur IA
- Développeur backend
- Ingénieur plateforme
- Ingénieur DevOps
- Architecte logiciel

Pré-requis

- Pratique de la programmation avec TypeScript et utilisation d'un terminal
- Compréhension des échanges HTTP, des API REST et des structures JSON
- Première expérience d'intégration d'un LLM par API et compréhension de l'appel d'outils
- Notions d'authentification, de gestion des secrets et d'autorisation avec OAuth

Pré-requis techniques

- Ordinateur sous Windows 11, macOS ou Linux avec 16 Go de RAM recommandés, processeur quatre cœurs et droits d'installation
- Environnement Node.js 22.19 ou supérieur avec npm, Git et Visual Studio Code installés
- Installation de MCP Inspector 2 et du SDK MCP TypeScript 2 avec dépendances figées dans l'environnement pédagogique
- Connexion Internet stable autorisant les services pédagogiques, les registres de paquets et les API utilisées, avec accès à un modèle de langage de test
- Pour le passage de l'examen, ordinateur compatible avec PSI Secure Browser, webcam, microphone et espace individuel calme, après validation du contrôle système

Programme de notre formation MCP fondamentaux : mise en pratique

[Jour 1 - Matin]

Fondamentaux MCP et repères de certification

- Présentation de la Formation Certification MCP fondamentaux : mise en pratique et des domaines de l'examen MCPA
- Rôle de MCP dans les systèmes agentiques et responsabilités des hôtes, clients et serveurs
- Primitives du protocole : outils, ressources, prompts et échanges JSON-RPC
- Différences entre MCP, API directes, plugins, RAG et communication interagents de type A2A
- Cas d'usage des agents de développement, données d'entreprise et outils opérationnels, écosystème et compromis d'adoption
- Atelier pratique : Explorer un serveur simple avec MCP Inspector, identifier ses capacités et interpréter ses échanges à partir de questions de préparation à MCPA.

[Jour 1 - Après-midi]

Clients MCP et intégration aux workflows LLM

- Responsabilités du client MCP, configuration des serveurs, métadonnées par requête et découverte facultative des capacités
- Invocation des outils, lecture des ressources et utilisation des modèles de prompts
- Intégration à une application LLM et articulation avec les frameworks d'agents
- Gestion de la compatibilité de version, validation des schémas, erreurs, nouvelles tentatives et serveurs indisponibles
- Permissions côté client, approbation utilisateur et analyse du cycle d'invocation pour l'examen
- Atelier pratique : Créer un client TypeScript connecté à un workflow LLM, appeler un outil et traiter une erreur de validation ainsi qu'une indisponibilité simulée.

[Jour 2 - Matin]

Serveurs MCP et exposition des systèmes externes

- Responsabilités du serveur MCP, capacités exposées, traitement indépendant des requêtes et exécution locale ou partagée
- Conception des schémas d'outils, interfaces de ressources, définitions de prompts et formats de sortie structurés
- Adaptation de fichiers, bases de données et API REST, GraphQL ou SaaS en capacités MCP
- Validation des entrées, effets de bord, idempotence, pagination, limites de débit et échecs partiels
- Authentification des services externes, moindre privilège et choix entre MCP, API directe, RAG et automatisation de workflows
- Atelier pratique : Construire un serveur exposant un outil et une ressource, intégrer une API simulée et vérifier la pagination, les entrées invalides et les erreurs du service.

[Jour 2 - Après-midi]

Sécurité, autorisation et gouvernance

- Analyse des frontières de confiance entre utilisateurs, clients, serveurs, outils et sources de données

- Distinction entre authentification et autorisation, gestion des secrets et autorisation HTTP avec OAuth
- Risques d'injection de prompt, d'empoisonnement des outils, de fuite de données et d'actions dangereuses
- Contrôles de consentement, approbation des actions sensibles, isolation d'exécution et application des politiques
- Revue de sécurité des serveurs et catalogues, pistes d'audit et raisonnement sur les scénarios de sécurité MCPA
- Atelier pratique : Ajouter l'authentification et des autorisations limitées à un serveur HTTP, imposer une approbation pour une action sensible et vérifier le refus d'un accès non autorisé.

[Jour 3 - Matin]

Protocole sans état, transports et extensions

- Modèle sans état de la révision 2026-07-28 : version, capacités et informations client par requête, découverte facultative et compatibilité avec les révisions antérieures
- Transports stdio et Streamable HTTP, réponses limitées à la requête, streaming et annulation
- Métadonnées HTTP et routage par en-têtes pour les passerelles, politiques et besoins d'observabilité
- État applicatif explicite par arguments et identifiants émis par le serveur, sans dépendance aux sessions de transport
- Interactions multi-allers-retours, traitements longs, catalogues avec indications de cache et frontières entre cœur du protocole et extensions
- Atelier pratique : Réaliser une interaction sans état avec découverte, métadonnées par requête et identifiant applicatif explicite, puis vérifier sa continuité sur deux instances de serveur.

[Jour 3 - Après-midi]

Fiabilisation, architecture et préparation à l'examen

- Inspection des échanges avec MCP Inspector et diagnostic des problèmes de transport, d'autorisation, de schéma et d'intégration au modèle
- Tests de contrat et de régression : schémas, versions, cas limites, pannes et évolution des outils, extensions et modèles
- Observabilité des intégrations : journaux applicatifs, traces, métriques et événements d'audit sans exposition des secrets
- Architectures locales, d'équipe et d'entreprise sans état, intégration au RAG, aux passerelles IA et aux workflows CI/CD
- Gouvernance des versions et catalogues, arbitrages de performance, coût, cache et fiabilité, feuille de route d'adoption et stratégie de préparation MCPA
- Atelier pratique : Diagnostiquer et instrumenter l'intégration construite, proposer son architecture de production et réaliser une évaluation blanche chronométrée avec correction argumentée.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes,

souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.