

Mis à jour le 11/06/2026

S'inscrire

Formation Azure AI Foundry

3 jours (21 heures)

Présentation

Microsoft AI Foundry vous aide à concevoir, tester et industrialiser des solutions d'IA générative sur l'écosystème Microsoft, du prototypage à la mise en production. Vous apprenez à structurer des cas d'usage (assistant métier, recherche documentaire, automatisation) avec une approche gouvernée, mesurable et sécurisée.

La formation se concentre sur la mise en œuvre opérationnelle : cadrage du besoin, choix des modèles, orchestration des prompts, RAG, évaluation et déploiement. Les participants manipulent les composants clés (catalogue de modèles, endpoints, gestion des secrets, observabilité) et appliquent les bonnes pratiques de sécurité, conformité et coûts.

L'approche est pratique via ateliers guidés et démos reproductibles : création d'un assistant, ingestion de données, mise en place de garde-fous, tests et monitoring. Les livrables incluent un mini-projet fonctionnel, des gabarits de prompts, une checklist de mise en production et un plan d'évaluation (qualité, latence, budget).

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

Objectifs

- Identifier et prioriser des cas d'usage IA générative adaptés au métier.
- Configurer un environnement AI Foundry et sécuriser l'accès aux ressources.
- Construire un flux RAG avec ingestion, indexation et recherche.
- Évaluer la qualité (tests, métriques) et itérer sur prompts et paramètres.
- Déployer, superviser et optimiser coûts/latence en conditions réelles.

Public visé

- Développeurs et ingénieurs logiciel
- Data/ML engineers et data scientists
- Architectes cloud / solutions
- Chefs de projet techniques / Product owners

Pré-requis

- Notions de Python ou JavaScript
- Compréhension des APIs REST et du format JSON
- Bases Azure (ressources, RBAC, réseau) ou équivalent cloud
- Notions d'IA générative (prompting, embeddings) appréciées

Pré-requis techniques

- Windows 11, macOS ou Linux (accès terminal)
- Navigateur récent et éditeur de code (ex. VS Code)
- Accès à un tenant Azure et droits de création de ressources
- Outils : Git, Azure CLI (ou équivalent) et accès réseau sortant HTTPS

Programme de notre formation Azure AI Foundry

[Jour 1 - Matin]

Découvrir Microsoft AI Foundry et cadrer un projet IA

- Positionnement d'AI Foundry dans l'écosystème Microsoft (Azure, modèles, outils)
- Identifier les cas d'usage : assistant interne, recherche documentaire, automatisation métier
- Choisir une approche : RAG, fine-tuning, agents, workflows
- Pré-requis projet : données, sécurité, contraintes de latence et de coût
- Atelier pratique : cadrer un cas d'usage et définir critères de succès (qualité, coût, délai).

[Jour 1 - Après-midi]

Créer son premier projet et exécuter des prompts de référence

- Créer un projet AI Foundry : ressources, environnements, rôles et accès
- Configurer un endpoint de modèle et les paramètres d'inférence (température, top_p, max tokens)
- Structurer des prompts : consignes, contexte, format de sortie, garde-fous
- Mettre en place des tests manuels : jeux d'exemples, critères d'acceptation, traces
- Atelier pratique : construire un prompt "assistant métier" avec sorties JSON et tests de non-régression.

[Jour 2 - Matin]

RAG : ingestion documentaire et recherche sémantique

- Préparer les sources : PDF/HTML/SharePoint, nettoyage, dédoublonnage, métadonnées
- Stratégies de chunking : taille, overlap, structure (titres, sections)
- Embeddings et indexation : choix du modèle, dimension, coût, rafraîchissement
- Requêtage : top-k, filtres, reranking, citations et traçabilité
- Atelier pratique : créer un mini-RAG sur un corpus interne et valider la qualité des réponses avec sources.

[Jour 2 - Après-midi]

Évaluation, observabilité et optimisation coût/latence

- Définir des métriques : exactitude, complétude, groundedness, taux d'hallucination
- Mettre en place une évaluation : jeux de tests, scoring, comparaison de versions
- Observabilité : logs, traces, prompts versionnés, analyse des erreurs récurrentes
- Optimiser : caching, réduction de contexte, choix de modèles, quotas et budgets
- Atelier pratique : benchmarker 2 configurations (prompt + RAG) et choisir la meilleure selon coût/qualité.

[Jour 3 - Matin]

Agents et outillage : automatiser des tâches avec des fonctions

- Concevoir un agent : objectifs, mémoire, outils, limites et règles de sécurité
- Définir des tools/fonctions : schémas d'entrée/sortie, validation, erreurs
- Orchestration : enchaînement d'étapes, gestion des reprises, idempotence
- Garde-fous : restrictions d'actions, validation humaine, politiques d'exécution
- Atelier pratique : créer un agent qui interroge une API métier et génère un compte-rendu structuré.

[Jour 3 - Après-midi]

Mise en production : sécurité, conformité et déploiement

- Sécurité : gestion des secrets, RBAC, isolation réseau, principes du moindre privilège
- Conformité : données sensibles, rétention, journalisation, politiques d'usage
- Packaging et déploiement : environnements, configuration, versioning, rollback
- Run : supervision, alerting, gestion des incidents, amélioration continue via feedback
- Atelier pratique : préparer un plan de mise en production (checklist sécurité + pipeline de déploiement + suivi KPI).

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.