

Mis à jour le 22/04/2025

S'inscrire

Formation Microsoft Entra ID

2 jours (14 heures)

Présentation

La formation [Microsoft Entra ID](#) (Anciennement Azure AD) vous apprendra à gérer des accès et des identités basées sur le cloud. Vous pourrez accéder à différentes ressources externes comme Microsoft 365. Azure Active Directory est devenu Microsoft Entra ID en 2024 mais ses fonctionnalités restent sensiblement les mêmes.

Durant votre formation, vous saurez maîtriser l'environnement Entra ID avec Azure en mettant en place un annuaire. Découvrez l'ensemble des aspects proposés par les extensions d'Entra ID et [Entra Connect](#).

Contrôlez, gérez et supervisez les accès au sein de votre organisation. Suivre notre formation permettra à vos collaborateurs de monter en compétences dans le domaine du cloud.

Simple d'utilisation, Entra ID peut être intégré dans un grand choix de plates-formes et d'applications. Cette fonctionnalité pourrait être efficace pour vos différents types de projets.

Objectifs

- Comprendre les fondamentaux de Microsoft Entra ID et ses cas d'usage
- Gérer les utilisateurs, groupes, rôles et licences
- Sécuriser l'environnement avec MFA et Conditional Access
- Découvrir l'identité hybride avec Entra Connect
- Intégrer des applications SaaS dans votre écosystème Entra ID

Public visé

- Administrateurs systèmes / cloud
- Architectes IT
- Ingénieurs DevOps

- Chefs de projet technique
- Développeurs intégrant une solution d'authentification

Pré-requis

- Connaissances de base sur Microsoft Azure (concepts fondamentaux)
- Connaissance de base d'Active Directory (Comptes et groupes)
- Notions de sécurité et d'authentification

Pré-requis techniques

- Ordinateur avec connexion internet stable
- Compte Microsoft personnel (gratuit) ou professionnel Navigateur web moderne (Edge, Chrome recommandés)
- Un second appareil (smartphone) pour tester l'authentification
- Compte développeur Microsoft ou abonnement Azure avec droits administratifs

Programme de notre Formation Microsoft Entra ID

Introduction à Microsoft Entra ID

- Positionnement dans l'écosystème Microsoft 365 et Azure
- Différences entre Entra ID et Active Directory local
- Les éditions et fonctionnalités (Free, P1, P2)
- Vue d'ensemble des flux d'authentification
- Introduction aux scénarios multi-tenants et de migration

Création et configuration de l'environnement

- Structure d'un tenant Entra ID
- Ajout et vérification d'un nom de domaine personnalisé
- Tour d'horizon du portail d'administration
- Atelier pratique : Configuration d'un tenant de test, personnalisation de l'interface

Gestion des identités

- Création et gestion des utilisateurs
- Types de groupes et méthodes d'attribution
- Attribution de licences (directe vs basée sur les groupes)
- Atelier pratique : Création d'utilisateurs en graphique et via PowerShell, organisation en groupes, attribution de licences

Les fondamentaux de la sécurité

- Les méthodes d'authentification disponibles
- Configuration et déploiement de l'authentification multifacteur
- Paramètres de sécurité par défaut et bonnes pratiques
- Atelier pratique : Activation du MFA, test des méthodes principales, consultation des rapports de sécurité

Scénarios multi-tenants et fondamentaux de migration

- Concepts de base des environnements multi-tenants
- Cas d'usage pour les environnements multi-tenants (fusions, acquisitions, séparations)
- Introduction aux stratégies de migration entre tenants
- Considérations de licence et de sécurité
- Planification et phases d'une migration entre tenants
- Atelier pratique étendu : Analyse des scénarios de migration et élaboration d'une stratégie pour un cas fictif

Accès Conditionnel

- Principes fondamentaux du Conditional Access
- Création de politiques basées sur l'emplacement et le device
- Configuration des contrôles d'accès (bloquer, exiger MFA)
- Atelier pratique : Création de politiques d'accès conditionnel, tests et validation

Introduction à l'identité hybride

- Présentation de Microsoft Entra Connect
- Les modèles d'authentification (PHS, PTA, fédération)
- Atelier pratique : Planification d'un déploiement Entra Connect (simulation)

Intégration des applications avec focus multi-tenant

- Vue d'ensemble de la galerie d'applications
- Applications multi-tenants et partage entre tenants
- Configuration du SSO pour les applications multi-tenant
- Autorisation d'applications entre tenants
- Configuration du consentement administrateur
- Atelier pratique étendu : Intégration d'une application SaaS et configuration pour un accès multi-tenant

Migration entre tenants et continuité des services

- Outils et méthodes de migration entre tenants Entra ID
- Migration des utilisateurs, groupes et permissions
- Gestion des applications durant une migration
- Stratégies pour la coexistence temporaire

- Maintien des accès applicatifs pendant la transition
- Cas pratiques de migration réussie
- Gestion des identités externes pendant une migration
- Atelier pratique étendu : Simulation d'un plan de migration complet pour une application critique

Supervision et bonnes pratiques

- Scripts et automatisation spécifiques pour la gestion multi-tenant
- Atelier pratique simplifié : Manipulation d'un script préconçu pour la gestion multi-tenant

Conclusion et ressources

- Récapitulatif des points clés
- Ressources pour approfondir
- Questions/réponses finales

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.