

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : AZIA

Niveau : Moyen

intra

Mise à jour le 02/10/25

*tarif valable jusqu'au 31/12/2025

Prochaines sessions

Contactez-nous pour connaître nos futures sessions.

Pré-requis

- Connaissances générales en Active Directory et gestion des identités
- Notions d'administration Azure (AZ-900 conseillé, AZ-104 recommandé)

Objectifs

Objectifs pédagogiques :

- Comprendre l'architecture et les services d'Azure Active Directory (Azure AD)
- Gérer les utilisateurs, groupes, rôles et permissions
- Mettre en place l'authentification multifacteur et l'accès conditionnel
- Sécuriser l'accès aux applications et ressources Azure
- Mettre en œuvre une stratégie de gouvernance des identités

Objectifs opérationnels :

- Concevoir, configurer et administrer une infrastructure d'identité Azure complète : gérer les utilisateurs, groupes, rôles et permissions, déployer des politiques d'accès conditionnel et MFA, intégrer des applications via SSO et synchroniser les identités via Azure AD Connect.

Programme

Jour 1 - Gestion des identités et authentification

Introduction à Azure AD et son rôle dans Azure

Gestion des utilisateurs et groupes

Gestion des rôles et RBAC (Role-Based Access Control)

Authentification multifacteur (MFA) et Passwordless

Travaux pratiques

Créer des utilisateurs et groupes Azure AD

Configurer la MFA pour un groupe d'utilisateurs

Jour 2 - Sécurité, gouvernance et intégrations

Accès conditionnel et stratégies d'accès sécurisées

Identity Protection et détection des risques

Intégration des applications avec Azure AD (SSO, OAuth2, OpenID Connect)

Gestion des identités hybrides avec Azure AD Connect

Gouvernance des identités (PIM - Privileged Identity Management)

Travaux pratiques

Configurer une règle d'accès conditionnel pour protéger une application SaaS

Mettre en place PIM pour la gestion des rôles à privilèges