Formation Azure – Active Directory & Identity Management (Entra ID)

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : AZAD

Niveau : Moyen

intra

Mise à jour le 08/01/26

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base du cloud computing
- Notions générales de sécurité informatique
- Une première expérience Azure est recommandée

Objectifs

Objectifs pédagogiques :

- Comprendre les enjeux de la gestion des identités dans Azure
- Maîtriser les concepts fondamentaux d'Azure Active Directory
- Comprendre les mécanismes d'authentification et d'autorisation
- Connaître les bonnes pratiques de sécurisation des accès
- Appréhender l'IAM dans une stratégie cybersécurité globale

Objectifs opérationnels :

- Administrer les identités et groupes dans Azure
- Mettre en place une gestion des accès basée sur les rôles (RBAC)
- Configurer l'authentification forte (MFA)
- Définir et appliquer des politiques d'accès conditionnel
- Sécuriser les accès aux applications et ressources Azure

Programme

Jour 1 – Fondamentaux de l'IAM sur Azure

Introduction à l'IAM et à Azure AD

Enjeux de la gestion des identités dans le cloud
Azure AD / Microsoft Entra ID : rôle et architecture
Identités cloud vs identités hybrides
IAM et modèle Zero Trust

Gestion des identités et des groupes

Utilisateurs et groupes Azure AD
Groupes statiques et dynamiques
Synchronisation des identités (principe)
Bonnes pratiques d'organisation

Authentification et sécurité des comptes

Méthodes d'authentification
Authentification multifacteur (MFA)
Gestion des mots de passe
Sécurité des comptes à privilèges

Atelier pratique

Création et gestion d'utilisateurs et de groupes
Mise en place du MFA
Analyse des paramètres de sécurité existants

Jour 2 – Contrôle des accès, sécurité avancée et bonnes pratiques

Autorisation et RBAC

Différence authentification / autorisation

Formation Azure – Active Directory & Identity Management (Entra ID)

Rôles Azure et RBAC
Attribution des rôles aux ressources
Principe du moindre privilège

Accès conditionnel et protection des identités

Politiques d’accès conditionnel
Gestion des accès selon le contexte
Détection des connexions à risque
Sécurisation des accès aux applications

IAM, conformité et bonnes pratiques

Journalisation et audit des accès
Gouvernance des identités
Revue périodique des accès
IAM et exigences de conformité

Atelier pratique

Mise en place d’une politique d’accès conditionnel
Sécurisation d’une application Azure
Étude de cas IAM et restitution collective