Formation Administration des accès et de l'identité Microsoft

Durée :	4.0 jour(s)
Objectifs :	• Mettre en œuvre une solution de gestion des identités • Mettre en œuvre une solution d'authentification et de gestion des accès • Mettre en œuvre la gestion des accès pour les applications • Mettre en œuvre une stratégie de gouvernance des identités
Public :	Ingénieurs ou Administrateurs
Prérequis :	• Avoir des connaissances sur les pratiques de sécurité, les concepts d'identité tels que l'authentification, l'autorisation et l'annuaire actif, le déploiement des charges de travail Azure • Avoir suivi la formation Microsoft Azure Administrateur - AZ-104
Modalités et moyens pédagogiques	Démonstrations visuelles et pratiques à travers des exercices d'application et/ou des cas concrets des stagiaires. Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran. Portail web: maformation.vaelia.fr
Modalités d'évaluation	Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
Moyens d'encadrement	Un formateur expert spécialisé en Systèmes et Réseaux dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
Satisfaction globale :	/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Jour 1

Mise en œuvre d'une solution de gestion des identités

- Mettre en œuvre la configuration initiale d'Azure AD
- Créer, configurer et gérer les identités
- Mettre en œuvre et gérer les identités externes
- Mettre en œuvre et gérer l'identité hybride

Labs 1

- Lab 1a : Gérer les rôles des utilisateurs
- Lab 1b : Définition des propriétés à l'échelle du locataire
- Lab 1c : Attribution de licences aux utilisateurs
- Lab 1d : Restaurer ou supprimer des utilisateurs supprimés
- Lab 1e : Ajout de groupes dans Azure AD
- Lab 1f : Modification des attributions de licences de groupe
- Lab 1g : Modification des attributions de licences d'utilisateur
- Lab 1h : Configuration de la collaboration externe
- Lab 1i : Ajouter des utilisateurs invités à l'annuaire
- Lab 1j : Explorez les groupes dynamiques

Jour 2

Mise en œuvre d'une solution d'authentification et de gestion des accès

- Sécuriser les utilisateurs d'Azure AD avec MFA
- Gérer l'authentification des utilisateurs
- Planifier, mettre en œuvre et administrer l'accès conditionnel
- Gestion de la protection des identités Azure AD

Labs 2

- Lab 2a : Activation de la fonction MFA d'Azure AD
- Lab 2b : Configurer et déployer la réinitialisation du mot de passe en libre-service (SSPR)
- Lab 2c : Utilisation des paramètres de sécurité par défaut
- Lab 2d : Mise en œuvre de politiques d'accès conditionnel, de rôles et d'affectations
- Lab 2e : Configuration des contrôles de session d'authentification
- Lab 2f : Gestion des valeurs de verrouillage intelligent d'Azure AD
- Lab 2g : Activation de la politique de risque d'ouverture de session
- Lab 2h : Configuration de la politique d'enregistrement de l'authentification MFA d'Azure AD

Jour 3

Mise en œuvre de la gestion des accès pour les Apps

- Planifier et concevoir l'intégration des applications d'entreprise pour le SSO
- Mettre en œuvre et surveiller l'intégration des applications d'entreprise pour le SSO
- Mettre en œuvre l'enregistrement des applications

Labs 3

- Lab 3a : Mise en œuvre de la gestion des accès pour les applications
- Lab 3b : Créer un rôle personnalisé pour gérer l'enregistrement des applications
- Lab 3c : Enregistrer une application
- Lab 3d : Accorder le consentement de l'administrateur du locataire à une application
- Lab 3e : Ajouter des rôles d'application aux applications et recevoir des jetons

Jour 4

Planification et mise en œuvre d'une stratégie de gouvernance des identités

- Planifier et mettre en œuvre la gestion des droits
- Planifier, mettre en œuvre et gérer les révisions d'accès
- Planifier et mettre en œuvre l'accès privilégié
- Surveiller et maintenir Azure AD

Labs 4

- Lab 4a : Créer et gérer un catalogue de ressources avec les droits Azure AD

- Lab 4b : Ajout d'un rapport d'acceptation des conditions d'utilisation
- Lab 4c : Gérer le cycle de vie des utilisateurs externes avec la gouvernance d'identité Azure AD
- Lab 4d : Créer des examens d'accès pour les groupes et les applications
- Lab 4e : Configuration de PIM pour les rôles Azure AD
- Labo 4f : Attribution d'un rôle Azure AD dans PIM
- Labo 4g : Attribution de rôles de ressources Azure dans PIM
- Lab 4h : Connexion des données d'Azure AD à Azure Sentinel

Le contenu de cette formation prépare au passage de l'examen de certification SC-300 pour devenir Microsoft Certified: Identity and Access Administrator Associate. (Voucher de test non inclus)