Programme de cours
Microsoft Identity and Access Administrator

Durée :	4 jours soit 28 heures	Référence :	SC-300T00

Public visé :

Ce cours est destiné aux administrateurs qui ont ou auront des tâches d'administration d'identité et d'accès, et/ou qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion des accès pour les solutions Azure.
Cette formation est destinée aux administrateurs qui souhaitent passer la certification SC-300T00.

Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Avoir une compréhension des pratiques de sécurité et exigences de sécurité de l'industrie telles que la défense en profondeur, l'accès le moins privilégié, la responsabilité partagée et le modèle de confiance zéro.
- Etre familiarisés avec les concepts d'identité tels que l'authentification, l'autorisation et l'annuaire actif.
- Avoir une certaine expérience du déploiement de charges de travail Azure. Ce cours ne couvre pas les bases de l'administration Azure, mais le contenu du cours s'appuie sur ces connaissances en ajoutant des informations spécifiques à la sécurité.
- Avoir une certaine expérience des systèmes d'exploitation Windows et Linux et des langages de script est utile mais pas obligatoire. Les laboratoires du cours peuvent utiliser PowerShell et l'interface de ligne de commande.
- Avoir suivi la formation SC-900 "Les principes fondamentaux de la sécurité, de la conformité et de l'identité Microsoft" ou avoir les connaissances équivalentes.

Objectifs pédagogiques :

A l'issue de la formation, les apprenants auront acquis les compétences suivantes :

- Mettre en place une solution de gestion des identités
- Mettre en place une solution d'authentification et de gestion des accès
- Mettre en œuvre la gestion des accès pour les applications
- Planifier et mettre en œuvre une stratégie de gouvernance des identités

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant
Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.
Après
Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)
Enfin
Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 1 : Implémenter une solution de gestion des identités

- Implémenter la configuration initiale d'Azure AD
- Créer, configurer et gérer des identités
- Implémenter et gérer les identités externes
- Implémenter et gérer l'identité hybride

Module 2 : Implémenter une solution d'authentification et de gestion des accès

- Sécurisez l'utilisateur Azure AD avec MFA
- Gérer l'authentification des utilisateurs
- Planifier, mettre en œuvre et administrer l'accès conditionnel
- Gérer la protection des identités Azure AD

Module 3 : implémenter la gestion des accès pour les applications

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

Module 4 : Planifier et mettre en œuvre une stratégie de gouvernance des identités

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