

Administrateur des identités et des accès Microsoft (SC-300T00)

Durée: 4 jours

Public cible: Professionnel TI

À qui s'adresse cette formation ?

Ce cours s'adresse aux administrateurs des identités et des accès qui prévoient de passer l'examen de certification associé, ou qui effectuent des tâches d'administration des identités et des accès dans leur travail quotidien. Ce cours serait également utile à un administrateur ou à un ingénieur qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion des accès pour les solutions basées sur Azure, jouant ainsi un rôle essentiel dans la protection d'une organisation.

Objectifs de la formation

- Mettre en œuvre une solution de gestion des identités
- Implémenter 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

Description sommaire

Ce cours fournit aux professionnels IT des identités et des accès, ainsi qu'aux professionnels IT de la sécurité, les connaissances et les compétences nécessaires pour mettre en œuvre des solutions de gestion des identités basées sur Microsoft Azure AD et les technologies d'identité connectées. Ce cours comprend du contenu sur l'identité pour Azure AD, l'enregistrement des applications d'entreprise, l'accès conditionnel, la gouvernance d'identité et d'autres outils d'identité.

Contenu du plan de cours

Parcours d'apprentissage 1 : Mettre en œuvre une solution de gestion des identités

- Mettre en œuvre la configuration initiale de Microsoft Entra ID
- Créer, configurer et gérer les identités
-

Mettre en œuvre et gérer les identités externes

- Mettre en œuvre et gérer les identités hybrides

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

- Sécuriser Microsoft Entra utilisateurs avec l'authentification multifactorielle (MFA)
- Gérer l'authentification utilisateur
- Planifier, implémenter et administrer l'accès conditionnel
- Gérer la protection de l'identité Microsoft Entra

Parcours d'apprentissage 3 : Mettre en œuvre la gestion des accès pour les applications

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

Parcours d'apprentissage 4 : Planifier et mettre en œuvre une stratégie de gouvernance des identités

- Planifier et mettre en œuvre la gestion des droits d'utilisation
- Planifier, implémenter et gérer les révisions d'accès
- Planifier et mettre en œuvre l'accès privilégié
- Surveiller et maintenir Microsoft Entra ID

Parcours d'apprentissage 5 : Ateliers

- Gérer les rôles utilisateur
- Configurer et déployer la réinitialisation de mot de passe en libre-service (SSPR)
- Utiliser des étiquettes de sécurité pour implémenter l'accès conditionnel
- Gérer les ressources Azure à l'aide d'Azure RBAC
- Ajouter un locataire hybride avec Microsoft Entra Connect
- Accorder le consentement d'administrateur au niveau du locataire à une application
-

Sécuriser l'inscription des informations de sécurité des utilisateurs avec les méthodes d'authentification obligatoires

- Configurer l'authentification pour une application Azure App Service
- Créer et gérer un catalogue de ressources dans la gestion des droits d'utilisation de Microsoft Entra
- Ajouter des conditions aux termes d'utilisation et à l'acceptation
- Configurer et tester une stratégie d'accès conditionnel
- Configurer une stratégie de risque d'utilisateur de protection de l'identité Microsoft Entra
- Configurer et déployer une application personnalisée à l'aide d'un modèle de gouvernance de l'application
- Configurer les paramètres d'enregistrement et de gouvernance pour une application
- Déléguer l'administration d'identité
- Implémenter l'authentification multifactorielle (MFA)
- Créer une révision d'accès pour les groupes et les applications

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Les participants administrent progressivement les identités et les accès Microsoft à travers des exercices concrets inspirés de scénarios professionnels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à gérer les identités, sécuriser les accès, mettre en œuvre l'authentification et la gouvernance avec Microsoft Entra ID.

Animée par un formateur certifié Microsoft, la formation privilégie l'interactivité et le développement de compétences techniques directement transférables pour protéger efficacement les ressources et les utilisateurs en contexte professionnel.

Prérequis

Les étudiants qui réussissent auront une connaissance et une compréhension préalables de :

-

Des meilleures pratiques de sécurité et les 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.

- Être familier avec les concepts d'identité tels que l'authentification, l'autorisation et l'annuaire actif.
- Avoir une certaine expérience du déploiement des charges de travail Azure. Ce cours ne couvre pas les bases de l'administration de Azure, mais le contenu du cours s'appuie sur ces connaissances en ajoutant des informations spécifiques à la sécurité.
- 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 le CLI.

Recommandations

- Bases en gestion des identités et des accès (IAM) Connaissance de Microsoft Entra ID (Azure AD)
- Compréhension des concepts de sécurité (authentification, MFA, accès conditionnel)
- Notions des environnements Microsoft 365 ou Azure

Certifications

Ce cours s'adresse aux administrateurs des identités et des accès qui prévoient de passer l'examen de certification associé.