Microsoft Identity and Access Administrator

Description

Ce cours fournit aux professionnels IT de l'identité et de l'accès, ainsi qu'aux professionnels en sécurité IT, les connaissances et les compétences nécessaires pour mettre en œuvre des solutions de gestion d'identité basées sur Microsoft Azure AD et les technologies d'identité connectées.

Reference
SC-300T00
Contenu du cours
Module 1 : Mettre en œuvre une solution de gestion de l'identité

- Leçon 1: Implémenter la configuration initiale d'Azure AD
- Leçon 2: Créer, configurer et gérer les identités
- Leçon 3: Mettre en œuvre et gérer les identités externes
- Leçon 4: Mettre en œuvre et gérer l'identité hybride

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

- Leçon 1: Sécuriser l'utilisateur Azure AD avec MFA
- Leçon 2: Gérer l'authentification des utilisateurs
- Leçon 3: Planifier, mettre en œuvre et administrer l'accès conditionnel
- Leçon 4: Gérer la protection de l'identité AD Azure

Module 3 : Implémenter la gestion de l'accès pour les applications

- Leçon 1: Planifier et concevoir l'intégration de l'entreprise pour SSO
- Leçon 2: Implémenter et surveiller l'intégration d'applications d'entreprise pour SSO
- Leçon 3: Implémenter l'enregistrement des applications

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

- Leçon 1: Planifier et mettre en œuvre la gestion des droits
- Leçon 2: Planifier, mettre en œuvre et gérer les examens d'accès
- Leçon 3: Planifier et mettre en œuvre un accès privilégié
- Leçon 4: Surveiller et maintenir Azure AD

Lab / Exercices
Module 1 :

- Lab : Gérer les rôles des utilisateurs
- Lab : Paramétrage de l'environnement Microsoft 365
- Lab : Attribuer des licences aux utilisateurs
- Lab : Restaurer ou supprimer des utilisateurs supprimés
- Lab : Ajouter des groupes dans Azure AD
- Lab : Modifier les attributions de licences de groupe
- Lab : Modifier les attributions de licences utilisateur
- Lab : Configurer la collaboration externe

- Lab : Ajouter des utilisateurs invités à l'annuaire
- Lab : Explorer les groupes dynamiques

Module 2 :

- Lab : Activer Azure AD MFA
- Lab : Configurer et déployer la réinitialisation de mot de passe en libre-service (SSPR)
- Lab : Travailler avec les paramètres de sécurité par défaut
- Lab : mettre en œuvre des politiques d'accès conditionnel, des rôles et des attributions
- Lab : Configurer les contrôles de session d'authentification
- Lab : Gérer les valeurs de verrouillage intelligent Azure AD
- Lab : Activer la stratégie de risque de connexion
- Lab : Configurer la stratégie d'inscription d'authentification Azure AD MFA

Module 3 :

- Lab : Implémenter la gestion des accès pour les applications
- Lab : Créer un rôle personnalisé pour l'enregistrement de l'application de gestion
- Lab : Enregistrer une application
- Lab : Accorder le consentement de l'administrateur dans l'environnement Microsoft 365 à une application
- Lab : Ajouter des rôles d'application aux applications et recevoir des jetons

Module 4 :

- Lab : Créer et gérer un catalogue de ressources avec le droit Azure AD
- Lab : Ajouter un rapport d'acceptation des conditions d'utilisation
- Lab : Gérez le cycle de vie des utilisateurs externes avec la gouvernance des identités Azure AD
- Lab : Créer des révisions d'accès pour les groupes et les applications
- Lab : Configurer PIM pour les rôles Azure AD
- Lab : Attribuer un rôle Azure AD dans PIM
- Lab : Attribuer des rôles de ressources Azure dans PIM
- Lab : Connecter les données d'Azure AD à Azure Sentinel

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification SC-300 : Microsoft Identity and Access Administrator. Si vous souhaitez passer cet examen, merci de contacter notre secrétariat qui vous communiquera son prix et s'occupera de toutes les démarches administratives nécessaires pour vous

Profils des participants

- Administrateurs de l'identité et de l'accès qui prévoient passer l'examen de certification associé ou qui effectuent des tâches d'identité et d'accès dans leur travail quotidien
- Administrateur ou un ingénieur qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion d'accès pour les solutions basées sur Azure ou pour jouer un rôle essentiel dans la protection d'une organisation

Connaissances Préalables

- Les meilleures pratiques en matière 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 dans le déploiement des 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
- Une certaine expérience avec les systèmes d'exploitation Windows et Linux et les langages de script est utile, mais pas nécessaire. Les laboratoires de cours peuvent utiliser PowerShell et le CLI

Objectifs

- Mettre en œuvre une solution de gestion de l'identité
- Implémenter une solution d'authentification et de gestion de l'accès
- Implémenter la gestion de l'accès pour les applications
- Planifier et mettre en œuvre une stratégie de gouvernance identitaire

Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)
3000
Durée (Nombre de Jours)
4