Administrateur d’identité et de l’accès Microsoft (SC-300)

Description

Développez vos compétences avec Microsoft Entra et Azure

Dans un monde numérique en constante évolution, la gestion des identités devient un enjeu stratégique. La formation Administrateur d’identité et de l’accès Microsoft (SC-300) vous offre une expertise indispensable dans l’utilisation de Microsoft Entra, Azure et Microsoft 365. Grâce à ce cours, vous apprendrez à concevoir, déployer et superviser des solutions modernes de gestion des identités et des accès.

En suivant cette formation SC-300, vous saurez garantir un accès sécurisé aux applications d’entreprise, tout en facilitant l’expérience utilisateur grâce à l’authentification fluide. Vous découvrirez comment appliquer une gouvernance efficace avec Microsoft Entra ID, intégrer la vérification d’identité Microsoft Entra et gérer les identités externes via Microsoft Entra External ID. Vous maîtriserez également les techniques de dépannage, de surveillance et de reporting adaptées à tous les environnements hybrides ou cloud.

Une formation certifiante pour accélérer votre carrière

La formation Administrateur d’identité et de l’accès Microsoft (SC-300) prépare également à l’examen de certification officiel. Vous pourrez ainsi prouver vos compétences en implémentant les meilleures pratiques de sécurité et d’administration d’identité basées sur Azure et Microsoft 365.

Contenu du cours
Module 1 : Explorer l’identité dans Microsoft Entra ID

- Expliquer le paysage des identités
- Explorer la Confiance zéro avec l’identité
- Discuter de l’identité en tant que plan de contrôle
- Découvrir pourquoi nous avons une identité
- Définir l’administration des identités
- Contraster les systèmes d’identité décentralisée avec les systèmes d’identité centralisée
- Discuter des solutions de gestion des identités
- Expliquer Microsoft Entra Business to Business
- Comparer les fournisseurs d’identité Microsoft
- Définir la gestion des licences d’identité
- Explorer l’authentification
- Discuter de l’autorisation
- Expliquer l’audit dans l’identité

Module 2 : Implémenter la configuration initiale de Microsoft Entra ID

- Configurer la marque de l'entreprise
- Configurer et gérer les rôles Microsoft Entra
- Configurer la délégation à l'aide d'unités administratives
- Analyser les autorisations de rôle Microsoft Entra
- Configurer et gérer des domaines personnalisés
- Configurer les paramètres au niveau du locataire

Module 3 : Créer, configurer et gérer des identités

- Créer, configurer et gérer des identités
- Créer, configurer et gérer des groupes
- Configurer et gérer l'inscription des appareils
- Gérer les licences
- Créer des attributs de sécurité personnalisés
- Explorer la création automatique d'utilisateurs

Module 4 : Implémenter et gérer des identités externes

- Description de l'accès invité et des comptes interentreprises
- Gérer les collaborations externes
- Inviter des utilisateurs externes : individuellement et en bloc
- Gérer les comptes d'utilisateur externes dans l'ID Microsoft Entra
- Gestion des utilisateurs externes dans des charges de travail Microsoft 365
- Implémenter et gérer l'identité vérifiée Microsoft Entra
- Configurer les fournisseurs d'identité
- Implémenter des contrôles d'accès interlocataires

Module 5 : Implémenter et gérer l'identité hybride

- Planifier, concevoir et implémenter Microsoft Entra Connect
- Implémenter et gérer la synchronisation de hachage de mot de passe (PHS)
- Implémenter et gérer l'authentification directe (PTA)
- Implémenter et gérer la fédération
- Résoudre les erreurs de synchronisation
- Mettre en œuvre Microsoft Entra Connect Health
- Gérer Microsoft Entra Health

Module 6 : Sécurisez les utilisateurs Microsoft Entra avec l'authentification multifacteur

- Qu'est-ce que l'authentification multifacteur Microsoft Entra ?
- Planifiez votre déploiement de l'authentification multifacteur
- Configurer les méthodes d'authentification multifacteur

Module 7 : Gérer l'authentification utilisateur

- Administrer les méthodes d’authentification FIDO2 et sans mot de passe
- Explorer l’application Authenticator et les jetons OATH
- Implémenter une solution d’authentification basée sur Windows Hello Entreprise
- Déployer et gérer la protection par mot de passe
- Configurer des seuils de verrouillage intelligent
- Implémenter l'authentification Kerberos et basée sur un certificat dans Microsoft Entra ID
- Configurer l'authentification utilisateur Microsoft Entra pour les machines virtuelles

Module 8 : Planifier, implémenter et administrer l’accès conditionnel

- Planifier les paramètres de sécurité par défaut
- Planifier les stratégies d’accès conditionnel
- Implémenter des contrôles et des affectations de stratégie d’accès conditionnel
- Tester et résoudre les problèmes des stratégies d’accès conditionnel
- Implémenter des contrôles d’application
- Implémenter la gestion des sessions
- Implémenter l’évaluation continue de l’accès

Module 9 : Gérer Microsoft Entra Identity Protection

- Passer en revue les principes fondamentaux de Identity Protection
- Implémenter et gérer une stratégie de risque d’utilisateur
- Surveiller, examiner et corriger les utilisateurs à risque
- Implémenter la sécurité pour les identités de charge de travail
- Explorer Microsoft Defender pour Identity

Module 10 : Implémenter le Gestionnaire d’accès pour des ressources Azure

- Affecter des rôles Azure
- Configurer des rôles Azure personnalisés
- Créer et configurer des identités managées
- Accéder aux ressources Azure avec des identités managées
- Analyser les autorisations des rôles Azure
- Configurer des stratégies RBAC Azure Key Vault
- Récupérer des objets auprès d’Azure Key Vault
- Découvrir Gestion des autorisations Microsoft Entra

Module 11 : Déployer et configurer Accès global sécurisé Microsoft Entra

- Explorer Accès global sécurisé
- Déployer et configurer Accès Internet Microsoft Entra
- Déployer et configurer Accès privé Microsoft Entra
- Découvrir comment utiliser le tableau de bord pour piloter Accès global sécurisé
- Créer des réseaux distants pour les utiliser avec Accès global sécurisé
- Utiliser l’accès conditionnel avec Accès global sécurisé
- Explorer les journaux et les options de surveillance d’Accès global sécurisé

Module 12 : Planifier et concevoir l’intégration des applications d’entreprise pour l’authentification unique

- Découvrir des applications à l’aide de Microsoft Defender pour les applications Cloud et du rapport d’application des services de fédération Active Directory (AD FS)

- Configurer des connecteurs aux applications
- Concevoir et implémenter des rôles de gestion des applications
- Configurer des applications SaaS de galerie préintégrées
- Implémenter et gérer des stratégies pour les applications OAuth

Module 13 : Implémenter et surveiller l'intégration des applications d'entreprise pour l'authentification unique

- Implémenter des personnalisations de jetons
- Implémenter et configurer les paramètres de consentement
- Intégrer des applications locales à l'aide du proxy d'application Microsoft Entra
- Intégrer des applications SaaS personnalisées pour l'authentification unique
- Implémenter l'approvisionnement des utilisateurs basé sur les applications
- Surveiller et auditer l'accès aux applications d'entreprise intégrées à Microsoft Entra
- Créer et gérer des collections d'applications

Module 14 : Implémenter l'inscription d'application

- Planifier votre stratégie d'inscription d'application métier
- Implémenter l'inscription d'application
- Inscrire une application
- Configurer l'autorisation pour une application
- Accorder le consentement administrateur au niveau locataire à des applications
- Implémenter l'autorisation d'application
- Gérer et superviser une application à l'aide de la gouvernance des applications

Module 15 : Inscrire des applications à l'aide de Microsoft Entra ID

- Planifier une inscription d'application
- Explorer des objets d'application et des principaux de service
- Créer des inscriptions d'applications
- Configurer l'authentification d'application
- Configurer les autorisations d'API
- Créer des rôles d'application

Module 16 : Planifier et implémenter la gestion des droits d'utilisation

- Définir des packages d'accès
- Configurer la gestion des droits d'utilisation
- Configurer et gérer des organisations connectées
- Passer en revue les droits par utilisateur

Module 17 : Planifier, implémenter et gérer la révision d'accès

- Planifier des révisions d'accès
- Créer des révisions d'accès pour les groupes et les applications
- Créer et configurer des révisions d'accès par programmation
- Surveiller les résultats de la révision d'accès
- Automatiser les tâches de gestion de la révision d'accès
- Configurer des révisions d'accès récurrentes

Module 18 : Planifier et implémenter un accès privilégié

Module 19 : Surveiller et gérer Microsoft Entra ID

- Analyser et examiner les journaux de connexion pour résoudre les problèmes d'accès
- Examiner et surveiller les journaux d'audit Microsoft Entra
- Exporter les journaux vers un système de gestion des événements et des informations de sécurité tiers
- Analyser des classeurs et des rapports Microsoft Entra
- Surveiller la posture de sécurité avec le score d'identité sécurisée

Module 20 : Explorer les nombreuses fonctionnalités de Gestion des autorisations Microsoft Entra

- Une expérience complète pour tous les environnements cloud
- Obtenir des insights généraux dans le tableau de bord Gestion des autorisations
- Approfondir l'analyse grâce à l'onglet Analytics
- Obtenir une meilleure compréhension de votre environnement avec les rapports
- Analyser les données historiques avec l'onglet Audit
- Prendre des mesures en réponse aux résultats avec l'onglet Correction de Gestion des autorisations
- Adopter une approche plus proactive de la gestion avec une surveillance continue
- Gérer l'accès à Gestion des autorisations Microsoft Entra
- Exemple complet

Lab / Exercices

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

Examen

- Ce cours prépare à la certification SC-300 : Microsoft Identity and Access Administrator.

Profils des participants

- Administrateurs d'identité et d'accès
- Ingénieurs en sécurité informatique
- Consultants en solutions cloud
- Architectes de solutions Microsoft Azure
- Responsables de la gouvernance des accès

Connaissances Préalables

- Comprendre les bases de Microsoft Azure et Microsoft 365
- Maîtriser les concepts fondamentaux de sécurité informatique
- Avoir des notions sur l'administration des identités et des accès

Objectifs

- Implémenter la gestion des identités avec Microsoft Entra ID
- Configurer l'authentification multifacteur et l'accès conditionnel
- Gérer les accès externes avec Microsoft Entra External ID

- Superviser, dépanner et surveiller l'accès aux ressources
- Mettre en œuvre la gouvernance des identités
- Déployer des solutions d'identité hybride sécurisées
- Intégrer la vérification d'identité Microsoft Entra
- Protéger les applications avec des stratégies d'accès sécurisé

Description
Administrateur d’identité et de l’accès Microsoft (SC-300)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)
3000
Durée (Nombre de Jours)
4
Reference
SC-300T00