Microsoft Identity and Access Administrator – Formation intensive («SC300»)

Cette formation officielle de niveau intermédiaire permet d'apprendre à concevoir, implémenter et exploiter des systèmes de gestion des identités et des accès d'entreprise avec Microsoft Entra (Azure AD). Ce cours permet de se préparer à l'examen SC-300.

Durée: 3 jours
Prix : 3'400.– excl. 8.1% TVA
Documents : Support numérique officiel Microsoft et accès Microsoft Learn
Code officiel: SC-300

Contenu

Le contenu de cette formation intensive est basé sur le contenu de l'examen « SC-300: Microsoft Identity and Access Administrator ». Préparez-vous dès maintenant au cours avec les contenus Microsoft Learn. Lors des sessions journalières intensives avec nos experts, vous travaillerez avec les supports de formation officiels Microsoft (plus d'informations à la rubrique « méthodologie et didactique »).
Ce cours est une formation intensive (bloc de sessions journalières), si vous préférez suivre cette formation au format flexible (6 à 8 sessions virtuelles de 3 heures sur max. 4 semaines), cliquez ici.

Contenu de la formation :

Module 1 : Implémenter une solution de gestion des identités

Apprenez à créer et à gérer votre implémentation de Microsoft Entra (anciennement : Azure Active Directory (Azure AD)), puis à configurer les utilisateurs, les groupes et les identités externes que vous allez utiliser pour exécuter votre solution. Vous apprendrez également à configurer et à gérer une solution d'identité hybride.

Chapitres

- Configurer et gérer Microsoft Entra ID
- Créer, configurer et gérer des identités
- Implémenter et gérer des identités externes
- Mettre en œuvre et gérer les identités hybrides

Lab : Gérer les rôles d'utilisateur
Lab : Utilisation des propriétés du locataire
Lab : Attribution d'une licence à l'aide de l'appartenance au groupe
Lab : Configurer les paramètres de collaboration externe
Lab : Ajouter des utilisateurs invités au répertoire
Lab : Ajouter un fournisseur d'identité fédéré
Lab : Ajouter une identité hybride avec Microsoft Entra ID

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

Implémentez et administrez votre gestion des accès avec Microsoft Entra ID (Azure AD). Utilisez MFA, l'accès conditionnel et la protection des identités pour gérer votre solution d'identité.

Chapitres

- Planifier et mettre en œuvre l'authentification multifacteur (MFA)
- Gérer l'authentification utilisateur

- Planifier, implémenter et administrer l'accès conditionnel
- Gérer Microsoft Entra Identity Protection
- Implémenter le Gestionnaire d'accès pour des ressources Azure

Lab : Activer des stratégies de connexion et de risque utilisateur
Lab : Configurer une stratégie d'inscription d'authentification multifacteur Microsoft Entra ID
Lab : Utiliser Azure Key Vault pour les identités managées
Lab : Implémenter et tester une stratégie d'accès conditionnel
Lab : Gérer les valeurs de verrouillage intelligent Microsoft Entra ID
Lab : Attribuer des rôles de ressources Azure dans Privileged Identity Management
Lab : Authentification Microsoft Entra ID pour machines virtuelles Windows et Linux
Lab : Activer la réinitialisation de mot de passe en libre-service Microsoft Entra ID
Lab : Activer l'authentification multifacteur Microsoft Entra ID

Module 3 : Implémenter la gestion des accès pour les applications

Découvrez comment les applications peuvent et doivent être ajoutées à votre solution d'identité et d'accès par le biais de l'inscription des applications dans Microsoft Entra ID (Azure AD). Inscrivez et gérez une nouvelle application dans votre environnement.

Chapitres

- Planifier et concevoir l'intégration des applications d'entreprise pour l'authentification unique
- Implémenter et surveiller l'intégration des applications d'entreprise et configurer l'authentification unique
- Implémenter l'inscription d'application
- Inscrire des applications à l'aide de Microsoft Entra ID

Lab : Stratégies d'accès Defender for Cloud Apps
Lab : Inscrire une application
Lab : Implémenter la gestion des accès pour les applications
Lab : Accorder le consentement administrateur à une application au niveau du locataire

Module 4 : Planifier et implémenter une stratégie de gouvernance des identités

Concevez et implémentez une gouvernance des identités pour votre solution d'identité en utilisant les droits, les révisions d'accès, l'accès privilégié et en supervisant votre instance Microsoft Entra ID (Azure Active Directory (Azure AD)).

Chapitres

- Planifier et implémenter la gestion des droits d'utilisation
- Planifier, implémenter et gérer les révisions d'accès
- Planifier et implémenter un accès privilégié
- Surveiller et gérer Microsoft Entra ID
- Explorer les nombreuses fonctionnalités de gestion des autorisations Microsoft Entra

Lab : Créer des révisions d'accès pour utilisateurs internes et externes
Lab : Gérer le cycle de vie des utilisateurs externes dans les paramètres d'Microsoft Entra ID Identity Governance
Lab : Ajouter un rapport d'acceptation des conditions d'utilisation
Lab : Créer et gérer un catalogue de ressources dans la gestion des droits d'utilisation Microsoft Entra ID
Lab : Configurer Privileged Identity Management (PIM) pour les rôles Microsoft Entra ID
Lab : Explorer Microsoft Sentinel et utiliser des requêtes Kusto pour examiner les sources de données Microsoft Entra ID
Lab : Surveiller et gérer votre posture de sécurité avec le score d'identité sécurisée

Objectifs

- Implémenter et gérer des identités utilisateur
- Implémenter la gestion des authentifications et des accès
- Planifier et implémenter des identités de charge de travail
- Planifier et implémenter la gouvernance des identités

Méthodologie & Didactique

Ce cours est une formation intensive (bloc de sessions journalières), si vous préférez suivre cette formation au format flexible (6 à 8 sessions virtuelles de 3 heures sur max. 4 semaines), cliquez ici.

Formule d'apprentissage mixte de Digicomp :

- **Pre-study :** dès l'inscription à la formation, vous recevez un accès à Microsoft Learn et vous pouvez dès lors commencer individuellement à vous familiariser avec la matière. Nous vous conseillons de passer en revue toute la matière au moins une fois avant le cours et de vous concentrer plus en détail sur les passages où vous manquez le plus de connaissances.
- **After-study :** après la formation, vous continuez à avoir accès à Microsoft Learn. Vous pouvez ainsi continuer à apprendre et à vous exercer selon vos besoins afin de permettre un apprentissage plus durable et de vous préparer idéalement à l'examen de certification.

Public cible

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 est également utile aux administrateurs ou aux ingénieurs qui souhaitent se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion des accès pour les solutions basées sur Azure et jouant ainsi un rôle essentiel dans la protection d'une organisation.

Prérequis

- Connaissances des pratiques de sécurité et des exigences en matière de sécurité de l'industrie telles que la «defense in depth», «least privileged access», «shared responsibility» et «Zero Trust model».
- Être familier avec les concepts d'identité tels que l'authentification, l'autorisation et Active Directory
- 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. PowerShell et le CLI peuvent être utilisés pendant les exercices du cours.

Nous recommandons de suivre le cours suivant au préalable ou de vous assurer de posséder des connaissances équivalentes :

- Microsoft Security, Compliance, and Identity Fundamentals – Formation intensive («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Formation flexible («SC900V»)

Certification

Cette formation marque la première étape de préparation à l'**examen** :

« SC-300: Microsoft Identity and Access Administrator »

La réussite de cet examen permet de décrocher la **certification** :

« Microsoft Certified: Identity and Access Administrator Associate »

ATTENTION : L'examen ne se déroule pas dans le cadre de la formation, vous devrez vous y inscrire séparément. Pratiquer vos nouvelles connaissances en situation réelle augmente considérablement vos chances de réussite à l'examen, c'est pourquoi nous vous conseillons de ne pas passer l'examen tout de suite après votre formation, mais de prendre votre temps et de vous y inscrire lorsque vous serez prêt.

Inscription à l'examen

Vous avez la possibilité de vous inscrire à un examen que vous passerez soit dans un de nos centres de formation Digicomp, agréés centre de test Pearson Vue, à Lausanne ou Genève, soit depuis chez vous.

Chez Digicomp : Inscrivez-vous à l'examen directement sur le site de Pearson VUE et sélectionnez l'un de nos centres de formation Digicomp (Lausanne ou Genève). Vous pourrez ensuite choisir parmi les créneaux d'examen proposés dans nos centres.

Chez vous : Pour passer un examen depuis chez vous, vous devez vous inscrire en passant par ce lien.

Le prix de l'examen est de CHF 216.- (sous réserve de modification par l'éditeur).

Formations complémentaires

- Microsoft Cybersecurity Architect – Formation intensive («SC100»)

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-digital-transformation-technologies/cloud/cloud-security/cours-microsoft-identity-and-access-administrator-formation-intensive-sc-300