# Devenir certifié Microsoft Identity and Access Administrator Associate (SC-300)

## Date et durée

Code formation : SC-300-BIS
Durée : 5 jours
Nombre d'heures : 35 heures

## Formation avec certification

Microsoft Certified: Identity and Access Administrator Associate

## Description

Un **administrateur des identités et des accès** est un professionnel chargé de gérer les systèmes et les processus liés à l'identification des utilisateurs et à l'accès aux ressources d'un système ou d'un réseau. Son rôle est crucial pour la **sécurité informatique** d'une entreprise ou d'une organisation.
Dans cette formation, vous apprendrez à **concevoir, mettre en œuvre et gérer des systèmes de gestion des identités et des accès** avec Microsoft Azure AD. Vous commencerez votre 1ère journée avec les principes fondamentaux qui vous permettront de comprendre les concepts de la sécurité, de l'identité et de la conformité. Ensuite, pendant 4 jours, vous examinerez en détail les processus de gestion des identités et des accès pour les applications d'entreprise. Vous découvrirez également les méthodes utilisées pour fournir des expériences transparentes et des capacités de gestion en libre-service pour tous les utilisateurs. Enfin, vous apprendrez à **mettre en place un accès adaptatif et une gouvernance** pour vos solutions de gestion des identités et des accès afin de dépanner, de surveiller et d'établir des rapports sur votre environnement.
A l'issue de cette formation Microsoft Azure, vous serez en mesure de **passer l'examen SC-300 inclus dans notre offre**. La réussite de celui-ci vous permettra d'obtenir la certification *Microsoft Certified : Identity and Access Administrator Associate*.

## Objectifs

À l'issue de la **formation Microsoft SC-300**, vous atteindrez les objectifs de compétences suivants :

- expliquer les concepts de sécurité, de conformité et d'identité ;
- connaitre les fonctions liées à la gestion des identités avec Microsoft Azure AD en tant que composant de Microsoft Entra ;
- connaitre les fonctions de sécurité incluses dans les solutions Microsoft ;
- connaitre les fonctions de conformité incluses dans les solutions Microsoft ;
- intégrer la gestion des identités avec Azure AD ;
- intégrer la gestion de l'authentification et de l'accès ;
- intégrer la gestion des accès pour des applications ;
- planifier et introduire une gouvernance des identités avec Azure AD ;
- réussir l'examen SC-300 et obtenir la certification Microsoft Certified : Identity and Access Administrator Associate.

## Points forts

Une formation dispensée par un formateur expert et certifié Microsoft ; un programme officiel en français avec des labs informatique et le passage de l'examen SC-900 inclus dans notre offre.

- **Garantie de certification :** cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.

## Certification

Cette formation vous permet de passer l'examen SC-300 qui mène à la certification **Microsoft Certified : Identity and Access Administrator Associate**. Pour garantir votre réussite à cet examen, vous devez savoir effectuer les opérations techniques suivantes :

- mettre en œuvre les identités dans Azure AD ;
- mettre en œuvre la gestion de l'authentification et de l'accès ;
- mettre en œuvre la gestion de l'accès aux applications ;
- planifier et mettre en œuvre la gouvernance des identités dans Azure AD.

Pour conclure, la **certification Azure Identity and Access Administrator Associate** permet de se préparer à passer d'autres certifications orientées sur des rôles plus avancés.
En savoir + sur les certifications Azure

## Modalités d'évaluation

Travaux Pratiques

## Pré-requis

Suivre la **formation Microsoft SC-900** nécessite les prérequis suivants :

- connaitre les bonnes pratiques en matière de sécurité informatique, telles que la défense en profondeur, l'accès au moindre privilège, la responsabilité partagée et le modèle de confiance zéro ;
- connaitre les concepts d'identité tels que l'authentification, l'autorisation et Active Directory ;
- avoir une expérience en déploiement de charges de travail sur Azure ;
- avoir des compétences en administration des systèmes Windows et Linux ainsi que dans la programmation de scripts est un plus, mais ce n'est pas obligatoire.

## Public

**Cette formation s'adresse aux publics suivants :**

- toutes personnes qui utilisent les produits et les services Microsoft et qui souhaitent acquérir des connaissances avancées en matière de sécurité, de conformité et d'identité.
- les administrateurs qui effectuent des tâches liées à la gestion des identités et des accès dans leurs travail quotidien et ceux qui souhaitent se certifier ;
- les administrateurs et les ingénieurs qui souhaitent se spécialiser dans la conception de solutions d'identité et de systèmes de gestion d'accès avec Azure.

## Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système
Responsable sécurité informatique

## Programme

# Les fondamentaux de la sécurité, de la conformité et de l’identité *(SC-900|1 jour)*

## Module 1 : introduction aux concepts de sécurité, de conformité et d'identité

- Comprendre les concepts de sécurité et de conformité :
  - le modèle de responsabilité partagée ;
  - la défense en profondeur ;
  - le modèle de confiance zéro ;
  - le cryptage et le hachage ;
  - les concepts de conformité.
- Comprendre les concepts d'identité :
  - l'identité en tant que premier critère de sécurité ;
  - l'authentification ;
  - l'autorisation ;
  - les fournisseurs d'identité ;
  - L'annuaire Active Directory.

## Module 2 : présentation des fonctions d'identités avec Microsoft Azure AD en tant que composant de Microsoft Entra

- Comprendre les principaux services et les types d'identités d'Azure AD :
  - qu'est-ce que Azure AD ? ;
  - les identités Azure AD ;
  - l'identité hybride ;
  - les différents types d'identité externes.
- Comprendre les fonctions d'authentification d'Azure AD :
  - les différentes méthodes d'authentification ;
  - l'authentification multifactorielle ;
  - la réinitialisation du mot de passe en libre-service ;
  - les différentes fonctions de protection et de gestion des mots de passe.
- Comprendre les fonctions de gestion des accès d'Azure AD :
  - l'accès conditionnel ;
  - les avantages des rôles Azure AD ;
  - les avantages du contrôle d'accès basé sur les rôles.
- Comprendre les fonctions de gouvernance et de protection des identités d'Azure AD :
  - la gouvernance des identités ;
  - la gestion des droits des utilisateurs et les révisions d'accès ;
  - les fonctionnalités de la gestion des identités privilégiées (PIM) ;
  - la protection des identités.

## Module 3 : présentation des fonctions de sécurité des produits Microsoft

- Comprendre les principales fonctions de sécurité d'Azure :
  - la protection DDoS d'Azure ;
  - le pare-feu Azure ;
  - qu'est-ce qu'un pare-feu d'application web ? ;
  - la segmentation du réseau avec les réseaux virtuels Azure ;
  - les groupes de sécurité réseau d'Azure ;
  - le système Azure Bastion et l'accès aux machines virtuelles ;
  - les méthodes de cryptage des données.

- Comprendre les fonctions de gestion de sécurité d'Azure :
    - la gestion de la posture de sécurité dans le cloud ;
    - la solution Microsoft Defender pour le cloud ;
    - les fonctions de sécurité améliorées de Microsoft Defender pour le cloud ;
    - les règles de base de la sécurité sur Azure.
- Comprendre les fonctions de sécurité de Microsoft Sentinel :
    - les concepts de surveillance SIEM et SOAR ;
    - les avantages de Microsoft Sentinel pour la gestion intégrée des menaces.
- Comprendre le système de protection contre les menaces de Microsoft 365 Defender :
    - les services de Microsoft 365 Defender :
        - Microsoft Defender pour Office 365 ;
        - Microsoft Defender pour Endpoint ;
        - Microsoft Defender pour Cloud Apps ;
        - Microsoft Defender pour l'identité ;
- le portail Microsoft 365 Defender.

### Module 4 : présentation des fonctions de conformité des produits Microsoft

- Comprendre le fonctionnement du portail d'approbation des services de Microsoft et les principes de protection de la vie privée :
    - les offres du portail d'approbation des services ;
    - les principes de confidentialité de Microsoft.
- Comprendre les fonctions de gestion de la conformité de Microsoft Purview :
    - le portail de conformité de Microsoft Purview ;
    - le gestionnaire de conformité ;
    - l'utilisation et les avantages du score de conformité.
- Comprendre les fonctions de protection des informations et de gestion du cycle de vie des données de Microsoft Purview :
    - les fonctionnalités de classification des données ;
    - les avantages de l'explorateur de contenu et de l'explorateur d'activités ;
    - les labels de confidentialité et les stratégies de labellisation ;
    - la prévention des pertes de données (DLP) ;
    - la gestion des enregistrements ;
    - les stratégies de conservation, les étiquettes de conservation et les stratégies d'étiquettes de conservation.
- Comprendre les fonctions de risque interne de Microsoft Purview :
    - la gestion des risques internes ;
    - la conformité des communications ;
    - la séparation des informations ;
    - les fonctionnalités de gouvernance des ressources dans Azure ;
    - l'utilisation de Azure Policy ;
    - l'utilisation des Blueprints Azure ;
    - la gouvernance unifiée des données.

## L'administration des identités et des accès avec Azure AD *(SC-300|4 jours)*

### Module 1 : implémentation des identités dans Azure AD

- Configurer et gérer un locataire Azure AD :
    - la configuration et la gestion des rôles ;
    - la configuration de la délégation via les unités administratives ;
    - l'analyse des autorisations des rôles ;

    - la configuration et la gestion des domaines personnalisés ;
    - la configuration des paramètres au niveau du locataire.
- Créer, configurer et gérer les identités Azure AD :
    - la création, la configuration et la gestion des identités ;
    - la création, la configuration et la gestion des groupes ;
    - la configuration et la gestion de l'adhésion et de l'enrôlement des appareils, incluant la réécriture ;
    - l'attribution, la modification et la création de rapports sur les licences.
- Implémenter et gérer les identités externes :
    - la gestion des paramètres de collaboration externe ;
    - l'invitation des utilisateurs externes, individuellement ou en masse ;
    - la gestion des comptes utilisateurs externes dans Azure AD ;
    - la configuration des fournisseurs d'identité, y compris SAML ou WS-Fed.
- Implémenter et gérer une identité hybride :
    - la mise en place et la gestion d'Azure AD Connect ;
    - la mise en place et la gestion de la synchronisation dans le cloud d'Azure AD Connect ;
    - la mise en place et la gestion de la synchronisation du hachage des mots de passe (PHS) ;
    - la mise en place et la gestion de l'authentification directe (PTA) ;
    - la mise en place et la gestion de l'authentification unique transparente (SSO) ;
    - la mise en place et la gestion de la fédération, excluant les déploiements manuels d'AD FS ;
    - la mise en place et la gestion de Azure AD Connect Health ;
    - la résolution des erreurs de synchronisation.

### Module 2 : implémentation de l'authentification et de la gestion des accès

- Mettre en place l'authentification multifactorielle Azure (MFA) :
    - la planification du déploiement d'Azure MFA, excluant le serveur MFA ;
    - la configuration et le déploiement de la réinitialisation des mots de passe en libre-service ;
    - la gestion des paramètres MFA d'Azure et pour les utilisateurs ;
    - l'extension de l'AFM d'Azure AD aux appareils tiers et locaux ;
    - la surveillance de l'activité MFA d'Azure AD.
- Mettre en place l'authentification des utilisateurs Azure AD :
    - la planification de l'authentification ;
    - l'implémentation et la gestion des méthodes d'authentification ;
    - l'implémentation et la gestion de Windows Hello Enterprise ;
    - l'implémentation et la gestion de la protection par mot de passe et des verrouillages intelligents ;
    - l'implémentation de l'authentification basée sur les certificats ;
    - la configuration de l'authentification des utilisateurs Azure AD pour les machines virtuelles Windows et Linux sur Azure.
- Mettre en place l'accès conditionnel Azure AD :
    - la planification des stratégies d'accès conditionnel ;
    - l'implémentation des affectations de politiques d'accès conditionnel ;
    - l'implémentation des contrôles de la politique d'accès conditionnel ;
    - le test et le dépannage des stratégies d'accès conditionnel ;
    - l'implémentation de la gestion des sessions ;
    - l'implémentation des restrictions sur les appareils ;
    - l'implémentation de l'évaluation continue de l'accès ;
    - la création d'une politique d'accès conditionnel à partir d'un modèle.
- Gérer la protection de l'identité Azure AD :
    - l'implémentation et la gestion d'une politique de risque pour l'utilisateur ;
    - l'implémentation et la gestion d'une stratégie de connexion à risque ;
    - l'implémentation et la gestion d'une stratégie d'enregistrement MFA ;
    - la surveillance, l'investigation et la correction des utilisateurs à risque ;
    - l'implémentation de la sécurité pour les identités de charge de travail.

- Mettre en place le gestionnaire d'accès pour les ressources Azure :
    - l'attribution de rôles Azure et la configuration des rôles personnalisés ;
    - la création et la configuration d'identités gérées ;
    - l'utilisation des identités gérées pour accéder aux ressources Azure ;
    - l'analyse des autorisations des rôles Azure ;
    - la configuration des politiques et du système RBAC d'Azure Key Vault.

### Module 3: implémentation de la gestion des accès pour les applications

- Gérer et superviser l'accès aux applications via Microsoft Defender for Cloud Apps :
    - la détection et la gestion des applications ;
    - la configuration des connecteurs d'application ;
    - l'implémentation des restrictions d'application ;
    - l'utilisation du contrôle d'accès conditionnel aux applications ;
    - la création des politiques d'accès et de session ;
    - l'implémentation et la gestion des politiques pour les applications OAUTH.
- Gérer et superviser l'intégration des applications d'entreprise :
    - la configuration et la gestion du consentement de l'utilisateur et de l'administrateur ;
    - l'identification des applications via les rapports d'activité de l'application ADFS ;
    - la conception et l'implémentation de la gestion de l'accès aux applications ;
    - la conception et l'implémentation des rôles de gestion des applications ;
    - la surveillance et l'audit de l'activité dans les applications d'entreprise ;
    - la conception et l'intégration des applications locales via le proxy d'application Azure AD ;
    - la conception et l'intégration des applications SaaS ;
    - la fourniture et la gestion des utilisateurs, des groupes et des rôles sur les applications d'entreprise ;
    - la création et la gestion de collections d'applications.
- Planifier et mettre en œuvre les enregistrements d'applications :
    - la planification des inscriptions aux applications ;
    - l'implémentation des enregistrements d'applications ;
    - la configuration des autorisations d'accès aux applications ;
    - la planification et la configuration des autorisations d'application à plusieurs niveaux ;
    - la gestion et la supervision des applications via la gouvernance des applications.

### Module 4 : planification et intégration de la gouvernance des identités dans Azure AD

- Implémenter la gestion des droits d'utilisation :
    - la planification des droits ;
    - la création et la configuration de catalogues ;
    - la création et la configuration de paquets d'accès ;
    - la gestion des demandes d'accès ;
    - l'implémentation et la gestion des conditions d'utilisation ;
    - la gestion du cycle de vie des utilisateurs externes dans les paramètres de gouvernance des identités d'Azure AD ;
    - la configuration et la gestion des organisations connectées ;
    - la révision des droits utilisateurs via la gestion des droits utilisateurs d'Azure AD.
- Implémenter et gérer les révisions d'accès :
    - la planification des révisions d'accès ;
    - la création et la configuration des révisions d'accès pour les groupes et les applications ;
    - la création et la configuration de programmes de révision d'accès ;
    - la surveillance de l'activité des révisions d'accès ;
    - la réponse aux activités de révision d'accès, incluant les réponses automatisées et manuelles.
- Implémenter l'accès privilégié :
    - la planification et la gestion des rôles Azure dans la gestion des identités privilégiées (PIM), incluant les paramètres et les affectations ;

    - la planification et la gestion des ressources Azure dans PIM, incluant les paramètres et les affectations ;
    - la planification et la configuration des groupes d'accès privilégiés ;
    - la gestion des demandes PIM et le processus d'approbation ;
    - l'analyse de l'historique PIM et des rapports d'audit ;
    - la création et la gestion de comptes d'accès d'urgence.
- Surveiller Azure AD :
    - la conception d'une stratégie de surveillance d'Azure AD ;
    - l'analyse des logs de connexion, d'audit et de provisionnement via le Azure Active Directory Administration Center ;
    - la configuration des paramètres de diagnostic, incluant Log Analytics, les comptes de stockage et Event Hub ;
    - la surveillance d'Azure AD via Log Analytics, incluant les requêtes KQL ;
    - l'analyse d'Azure AD via les classeurs et les rapports du Centre d'administration Azure Active Directory ;
    - le contrôle et l'amélioration de la posture de sécurité via Secure Identity Score.

*Microsoft®, Microsoft Azure Active Directory®, Microsoft 365®, Microsoft Entra® et Power Platform® sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et dans d'autres pays.*