# *Administrateur d'identité et d'accès Microsoft*

## *Formation officielle Microsoft Azure SC-300 : Identity and Access Administrator*

### DESCRIPTION

Cette formation vous permettra de concevoir, implémenter et exploiter les systèmes de gestion des identités et des accès de l'organisation à l'aide d'Azure Active Directory.

Cette formation est orientée sur la gestion des accès, la gouvernance autour de la gestion des accès et des applications.

### OBJECTIFS PEDAGOGIQUES

- Implémenter une solution de gestion des identités
- Implémenter une solution de gestion des authentifications et des accès
- Implémenter la gestion des accès pour les applications
- Planifier et implémenter une stratégie de gouvernance des identités

### PUBLIC CIBLE

- Administrateurs
- Opérateurs de sécurité

### PRE-REQUIS

- Pour participer à cette formation, Il faut avoir préalablement suivi la formation « SC-900 : Microsoft Security, Compliance, and Identity Fundamentals » et la formation « AZ-104 : Azure Administrator » ou avoir un niveau équivalent.
- Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

### METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique du formateur, complétés de travaux pratiques et de mises en situation.

### PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es

**Stage pratique**
Sécurité

Code :
**SC300**

Durée :
**4 jour(s) (28,00 heures)**

Exposés : **40 %**
Cas pratiques : **40 %**
Echanges d'expérience : **20 %**

**Inter-entreprises :**
Prochaines sessions disponibles sur notre site web.
Tarif : 2 900,00 € HT / participant

**Intra-entreprise :**
Tarifs et dates sur demande.

d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

**MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION**

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

**PROGRAMME PEDAGOGIQUE DETAILLE**

***OUVERTURE DE SESSION***

- Accueil des participants et tour de table des attentes
- Présentation du déroulé de la formation

***IMPLÉMENTER LA CONFIGURATION INITIALE DE MICROSOFT ENTRA ID***

- Implémenter la configuration initiale de Microsoft Entra ID.
- Créer, configurer et gérer des identités.
- Implémenter et gérer des identités externes (à l’exception des scénarios B2C).
- Implémenter et gérer l’identité hybride.

***CRÉER, CONFIGURER ET GÉRER DES IDENTITÉS***

- Créer, configurer et gérer des identités.
- Créer, configurer et gérer des groupes.
- Gérer les licences.
- Expliquer les attributs de sécurité personnalisés et le provisionnement automatique d’utilisateurs.

***IMPLÉMENTER ET GÉRER LES IDENTITÉS EXTERNES***

- Gérer les paramètres de collaboration externe dans Microsoft Entra ID.
- Inviter des utilisateurs externes (individuellement ou en bloc).
- Gérer les comptes d’utilisateur externes dans l’ID Microsoft Entra.
- Configurer les fournisseurs d’identité (social et SAML/WS-FED).

***IMPLÉMENTER ET GÉRER L'IDENTITÉ HYBRIDE***

- Planifier, concevoir et mettre en œuvre Microsoft Entra Connect.
- Gérer Microsoft Entra Connect.
- Gérer la synchronisation de hachage de mot de passe (PHS).
- Gérer l'authentification directe (PTA).
- Gérer l'authentification unique transparente.
- Gérer la fédération en excluant les déploiements ADFS manuels.
- Résoudre les erreurs de synchronisation.
- Implémenter et gérer Microsoft Entra Connect Health.

***IMPLÉMENTER LA CONFIGURATION INITIALE DE MICROSOFT ENTRA ID***

- Implémenter la configuration initiale de Microsoft Entra ID.
- Créer, configurer et gérer des identités.
- Implémenter et gérer des identités externes (à l'exception des scénarios B2C).
- Implémenter et gérer l'identité hybride.

***SÉCURISER LES UTILISATEURS MICROSOFT ENTRA AVEC L'AUTHENTIFICATION MULTIFACTEUR***

- Découvrir l'authentification multifacteur Microsoft Entra.
- Créer un plan pour déployer l'authentification multifacteur Microsoft Entra.
- Activer l'authentification multifacteur Microsoft Entra pour les utilisateurs et les applications spécifiques.

***GÉRER L'AUTHENTIFICATION UTILISATEURS***

- Administrer les méthodes d'authentification (FIDO2/sans mot de passe).
- Implémenter une solution d'authentification basée sur Windows Hello Entreprise.
- Configurer et déployer la réinitialisation du mot de passe en libre-service.
- Déployer et gérer la protection par mot de passe.
- Implémenter et gérer les restrictions de locataire.

***PLANIFIER, IMPLÉMENTER ET ADMINISTRER L'ACCÈS CONDITIONNEL***

- Planifier et implémenter les paramètres de sécurité par défaut.
- Planifier des stratégies d'accès conditionnel.
- Implémenter des contrôles et des affectations de stratégie d'accès conditionnel (ciblage applications et conditions).
- Tester et résoudre les problèmes des stratégies d'accès conditionnel.
- Implémenter des contrôles d'application.
- Implémenter la gestion des sessions.
- Configurer des seuils de verrouillage intelligent.

***GÉRER MICROSOFT ENTRA IDENTITY PROTECTION***

- Implémenter et gérer une stratégie de risque d'utilisateur.

- Implémenter et gérer des stratégies de risque de connexion.
- Implémenter et gérer la stratégie d'inscription MFA.
- Surveiller, examiner et corriger les utilisateurs à risque.

***IMPLÉMENTER LE GESTIONNAIRE D'ACCÈS POUR DES RESSOURCES AZURE***

- Configurer et utiliser les rôles Azure dans Microsoft Entra ID.
- Configurer une identité managée et l'affecter à des ressources Azure.
- Analyser les autorisations de rôle accordées à un utilisateur ou héritées par celui-ci.
- Configurer l'accès aux données dans Azure Key Vault en utilisant une stratégie RBAC.

***PLANIFIER ET CONCEVOIR L'INTÉGRATION DES APPLICATIONS D'ENTREPRISE POUR L'AUTHENTIFICATION UNIQUE***

- Découvrir des applications à l'aide des applications Defender pour le cloud ou du rapport sur les applications ADFS.
- Concevoir et implémenter la gestion des accès pour les applications.
- Concevoir et implémenter des rôles de gestion des applications.
- Configurer des applications SaaS (de galerie) pré-intégrées.

***IMPLÉMENTER ET SURVEILLER L'INTÉGRATION DES APPLICATIONS D'ENTREPRISE POUR L'AUTHENTIFICATION***

- 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 d'applications.
- Superviser et auditer l'accès/l'authentification pour les applications d'entreprise intégrées à Microsoft Entra ID.

***IMPLÉMENTER L'INSCRIPTION D'APPLICATION***

- Planifier votre stratégie d'inscription d'application métier.
- Implémenter les inscriptions d'applications.
- Configurer des autorisations de l'application.
- Planifier et configurer les autorisations d'application multiniveau.

***ENREGISTRER DES APPLICATIONS À L'AIDE DE MICROSOFT ENTRA ID***

- Expliquer les avantages de l'enregistrement des applications dans Microsoft Entra ID.
- Comparer et contraster les applications uniques et multi-

locataires.
- Décrire ce qui se passe et les principaux paramètres lors de l'enregistrement d'une application.
- Décrire la relation entre les objets d'application et les principaux de service.

***PLANIFIER ET IMPLÉMENTER LA GESTION DES DROITS D'UTILISATION***

- Définir des catalogues.
- Définir des packages d'accès.
- Planifier, implémenter et gérer des droits d'utilisation.
- Implémenter et gérer les conditions d'utilisation.
- Gérer le cycle de vie des utilisateurs externes dans les paramètres Gouvernance des ID Microsoft Entra.

***PLANIFIER, IMPLÉMENTER ET GÉRER LA RÉVISION D'ACCÈS***

- Planifier des révisions d'accès.
- Créer des révisions d'accès pour les groupes et les applications.
- Surveiller les résultats de la révision d'accès.
- Gérer les licences pour les révisions d'accès.
- Automatiser les tâches de gestion pour la révision d'accès.
- Configurer des révisions d'accès récurrentes.

***PLANIFIER ET IMPLÉMENTER UN ACCÈS PRIVILÉGIÉ***

- Définir une stratégie d'accès privilégié pour les utilisateurs administratifs (ressources, rôles, approbations et seuils).
- Configurer Privileged Identity Management pour les rôles Microsoft Entra.
- Configurer Privileged Identity Management pour les rôles Azure.
- Attribuer des rôles.
- Gérer les demandes PIM.
- Analyser l'historique et les rapports d'audit PIM.
- Créer et gérer des comptes d'accès d'urgence.

***SURVEILLER ET GÉRER MICROSOFT ENTRA ID***

- Analyser et investiguer les journaux de connexion pour résoudre les problèmes d'accès.
- Examiner et surveiller les journaux d'audit Microsoft Entra.
- Activer et intégrer des journaux de diagnostic Microsoft Entra à Log Analytics/Azure Sentinel.
- Exporter les journaux de connexion et d'audit vers un outil SIEM tiers.
- Passer en revue les activités Microsoft Entra à l'aide de Log Analytics/Azure Sentinel, en excluant l'utilisation du langage de requête Kusto (KQL).
- Analyser les classeurs et les rapports Microsoft Entra.
- Configurer les notifications.

***EXPLORER LES NOMBREUSES FONCTIONNALITÉS DE MICROSOFT ENTRA***

***PERMISSIONS MANAGEMENT***

- Comprendre les fonctionnalités de Microsoft Entra Permissions Management.
- Découvrir plus en détail comment la gestion des autorisations vous permet de découvrir, de corriger et de surveiller les identités, les autorisations et les ressources.
- Obtenir des vues réelles des données et des analyses fournies par la gestion des autorisations.

***CLÔTURE DE SESSION***

- Revue des principaux concepts clés présentés lors de la formation
- Échange autour des questions et réponses additionnelles

**Accessibilité**

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com