Programme de formation SC-300 : Microsoft Identity and Access Administrator

(Préparation certification Microsoft SC-300)

DESCRIPTION DE LA FORMATION :

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 :

A l'issue de cette formation, les participants seront en capacité de :

- Explorer l'identité et Azure AD
- Implémenter la configuration initiale d'Azure Active Directory
- Créer, configurer et gérer des identités
- Implémenter et gérer des identités externes
- Implémenter et gérer une identité hybride
- Sécuriser les utilisateurs Azure Active Directory avec l'authentification multifacteur
- Gérer l'authentification utilisateur
- Planifier, implémenter et administrer l'accès conditionnel
- Gérer Azure AD Identity Protection
- Implémenter le Gestionnaire d'accès pour des ressources Azure
- Planifier et concevoir l'intégration des applications d'entreprise pour l'authentification unique
- Implémenter et surveiller l'intégration des applications d'entreprise pour l'authentification unique
- Implémenter l'inscription d'application
- Planifier et implémenter la gestion des droits d'utilisation
- Planifier, implémenter et gérer la révision d'accès
- Planifier et implémenter un accès privilégié
- Surveiller et gérer les Azure Active Directory

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours officiel Microsoft sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un formateur expérimenté et accrédité Microsoft Certified Trainer.
- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.

- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Explorer l'identité et Azure AD

- Définir les termes d'identité courants et expliquer leur utilisation dans Microsoft Cloud.
- Explorer les outils de gestion courants et les besoins d'une solution d'identité.
- Passer en revue l'objectif de Confiance zéro et comment il est appliqué dans Microsoft Cloud.
- Explorer les services d'identité disponibles dans Microsoft Cloud.

Implémenter la configuration initiale d'Azure Active Directory

- Implémenter la configuration initiale d'Azure Active Directory.
- 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 et des groupes.
- Gérer les licences.
- Expliquer les attributs de sécurité personnalisés et le provisionnement automatique d'utilisateurs.

Implémenter et gérer des identités externes

- Gérer les paramètres de collaboration externe dans Azure Active Directory.
- Inviter des utilisateurs externes (individuellement ou en bloc).
- Gérer les comptes d'utilisateurs externes dans Azure Active Directory.
- Configurer les fournisseurs d'identité (social et SAML/WS-FED).

Implémenter et gérer une identité hybride

- Planifier, concevoir et implémenter des Azure Active Directory Connect (AADC).
- Gérer Azure Active Directory Connect (AADC).
- Gérer la synchronisation de hachage de mot de passe (PHS).
- Gérer l'authentification directe (PTA).
- Gérer l'authentification unique transparente (authentification unique transparente).
- Gérer la fédération en excluant les déploiements ADFS manuels.
- Résoudre les erreurs de synchronisation.
- Implémenter et gérer des Azure Active Directory Connect Health.

Sécuriser les utilisateurs Azure Active Directory avec l'authentification multifacteur

- Découvrir Azure AD Multi-Factor Authentication (Azure AD MFA).
- Créer un plan pour déployer Azure AD MFA.
- Activer Azure AD MFA pour les utilisateurs et des applications spécifiques.

Gérer l'authentification utilisateur

- 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.
- 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 Azure AD Identity Protection

- Implémenter et gérer une stratégie de risque d'utilisateur et 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 des rôles Azure dans Azure AD.
- 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 de MCAS ou du rapport d'application ADFS.
- Concevoir et implémenter la gestion des accès pour les applications.
- Concevoir et implémenter des rôles de gestion des applications.
- Configurer des applications SaaS (galerie) pré-intégrées.

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 Azure AD.
- Intégrer des applications SaaS personnalisées pour l'authentification unique.
- Implémenter l'approvisionnement des utilisateurs d'applications.
- Surveiller et auditer l'accès/l'authentification pour les applications d'entreprise intégrées Azure Active Directory.

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.

Planifier et implémenter la gestion des droits d'utilisation

- Définir des catalogues et les 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 d'Azure AD Identity Governance.

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.
- Configurer Privileged Identity Management pour les rôles Azure et Azure AD.
- 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 les Azure Active Directory

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

PRÉREQUIS :

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

PRE-CERTIFCIATION :

Cette formation prépare à l'examen de certification Microsoft SC-300 Microsoft Identity and Access Administrator »

DUREE : 4 jours (28 heures)

INTERLOCUTEURS : Administrateurs, opérateurs de sécurité

NIVEAU : Intermédiaire