Programme de cours
Configurer et gérer les droits d'accès avec Microsoft Entra ID.

Durée :	1 jour soit 7 heures	Référence :	SC-5008

Public visé :

Le public concerné par cette formation "Configurer et gérer les droits d'accès avec Microsoft Entra ID" est principalement constitué de professionnels travaillant dans des rôles liés à la sécurité informatique et à la gestion des identités dans des environnements Azure. Voici quelques profils typiques :

- **Administrateurs Azure** : Ceux qui gèrent les ressources et les services Azure, en particulier la gestion des identités et des accès au sein d'Azure Active Directory.
- **Responsables de la sécurité informatique** : Les professionnels chargés de mettre en place des stratégies de sécurité et de conformité dans un environnement Azure, en veillant à la gestion des droits d'accès et à la protection des ressources sensibles.
- **Architectes de solutions cloud** : Ceux qui conçoivent et mettent en œuvre des solutions sécurisées dans le cloud, utilisant Microsoft Entra pour gérer les accès aux services Azure.
- **Consultants en gestion des identités et des accès** : Les experts qui accompagnent les entreprises dans la mise en place de stratégies d'accès sécurisées, en particulier dans un environnement hybride ou multi-cloud.
- **Responsables de la gouvernance et de la conformité** : Les professionnels qui assurent le respect des politiques et des normes de conformité, comme celles relatives à la gestion des accès privilégiés et des revues d'accès.

Pré-requis :

- Connaissances de base en administration Azure.
- Capacité à créer des utilisateurs et des groupes avec Microsoft Entra.

Objectifs pédagogiques :

- **Maîtriser la gestion des droits d'accès** en attribuant rapidement les droits d'accès aux utilisateurs internes et externes, en configurant des packages d'accès et en gérant le cycle de vie des utilisateurs.
- **Acquérir les compétences nécessaires pour planifier et mettre en œuvre des revues d'accès** pour garantir une gouvernance appropriée, y compris la création de programmes de revue d'accès et l'automatisation des tâches associées.
- **Appliquer des stratégies de surveillance et d'analyse des événements d'accès** en utilisant les journaux d'audit et de diagnostic pour résoudre les problèmes d'accès et maintenir la sécurité de l'environnement Azure.
- **Configurer et gérer l'accès privilégié** avec Microsoft Entra, en définissant des stratégies d'accès privilégié, en utilisant Privileged Identity Management (PIM) et en supervisant les rôles administratifs pour renforcer la sécurité des ressources Azure.
- **Découvrir et exploiter les fonctionnalités avancées de Microsoft Entra Permissions Management** pour surveiller, analyser et remédier aux permissions, tout en optimisant la gestion des accès dans un environnement cloud sécurisé.

Compétences acquises à l'issue de la formation :

- Maîtriser la gestion des droits d'accès en attribuant rapidement les droits d'accès aux utilisateurs internes et externes, en configurant des packages d'accès et en gérant le cycle de vie des utilisateurs.
- Acquérir les compétences nécessaires pour planifier et mettre en œuvre des revues d'accès pour garantir une gouvernance appropriée, y compris la création de programmes de revue d'accès et l'automatisation des tâches associées.
- Appliquer des stratégies de surveillance et d'analyse des événements d'accès en utilisant les journaux d'audit et de diagnostic pour résoudre les problèmes d'accès et maintenir la sécurité de l'environnement Azure.
- Configurer et gérer l'accès privilégié avec Microsoft Entra, en définissant des stratégies d'accès privilégié, en utilisant Privileged Identity Management (PIM) et en supervisant les rôles administratifs pour renforcer la sécurité des ressources Azure.
- Découvrir et exploiter les fonctionnalités avancées de Microsoft Entra Permissions Management pour surveiller, analyser et remédier aux permissions, tout en optimisant la gestion des accès dans un environnement cloud sécurisé.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Programme de cours
Configurer et gérer les droits d'accès avec Microsoft Entra ID.

Description / Contenu

Utilisez Microsoft Entra pour gérer l'accès en utilisant les droits d'accès, les revues d'accès, les outils d'accès privilégié et surveiller les événements d'accès.

Module 1 : Planifier et mettre en œuvre la gestion des droits d'accès.
Lorsque de nouveaux utilisateurs ou des utilisateurs externes rejoignent votre site, leur attribuer rapidement l'accès aux solutions Azure est essentiel. Explorez comment attribuer des droits d'accès aux utilisateurs pour qu'ils puissent accéder à votre site et à vos ressources.

- Définir les packages d'accès
- Exercice : Créer et gérer un catalogue de ressources avec la gestion des droits d'accès Microsoft Entra
- Configurer la gestion des droits d'accès
- Exercice : Ajouter un rapport d'acceptation des conditions d'utilisation
- Exercice : Gérer le cycle de vie des utilisateurs externes avec la gouvernance des identités Microsoft Entra
- Configurer et gérer les organisations connectées
- Examiner les droits d'accès par utilisateur

Module 2 : Planifier, mettre en œuvre et gérer la revue des accès.
Une fois l'identité déployée, une gouvernance appropriée à l'aide des revues d'accès est nécessaire pour garantir une solution sécurisée. Explorez comment planifier et mettre en œuvre des revues d'accès.

- Planifier les revues d'accès
- Créer des revues d'accès pour les groupes et les applications
- Créer et configurer des programmes de revue d'accès
- Surveiller les résultats des revues d'accès
- Automatiser les tâches de gestion des revues d'accès
- Configurer des revues d'accès récurrentes

Module 3 : Surveiller et maintenir Microsoft Entra ID.
Les journaux d'audit et de diagnostic dans Microsoft Entra ID offrent une vue détaillée sur la manière dont les utilisateurs accèdent à votre solution Azure. Apprenez à surveiller, résoudre les problèmes et analyser les données de connexion.

- Analyser et enquêter sur les journaux de connexion pour résoudre les problèmes d'accès
- Examiner et surveiller les journaux d'audit Microsoft Entra
- Exercice : Connecter les données de Microsoft Entra ID à Microsoft Sentinel
- Exporter les journaux vers un système de gestion des informations et des événements de sécurité tiers
- Analyser les tableaux de bord et les rapports Microsoft Entra
- Surveiller la posture de sécurité avec le score de sécurité de l'identité

Module 4 : Planifier et mettre en œuvre l'accès privilégié.
Assurer la protection et la gestion des rôles administratifs pour renforcer la sécurité de votre solution Azure est essentiel. Explorez comment utiliser PIM (Privileged Identity Management) pour protéger vos données et ressources.

- Définir une stratégie d'accès privilégié pour les utilisateurs administratifs
- Configurer Privileged Identity Management pour les ressources Azure
- Exercice : Configurer Privileged Identity Management pour les rôles Microsoft Entra
- Exercice : Assigner des rôles Microsoft Entra dans Privileged Identity Management
- Exercice : Assigner des rôles de ressources Azure dans Privileged Identity Management
- Planifier et configurer les groupes d'accès privilégiés
- Analyser l'historique des audits et les rapports de Privileged Identity Management
- Créer et gérer des comptes d'accès d'urgence

Module 5 : Explorez les nombreuses fonctionnalités de Microsoft Entra Permissions Management.
En explorant plus en détail les fonctionnalités de Microsoft Entra Permissions Management, nous utilisons le cadre de découverte, remédiation, surveillance comme guide pour expliquer comment les fonctionnalités de Permissions Management peuvent bénéficier à votre organisation.

- Une expérience complète pour tous les environnements cloud
- Obtenez des aperçus de haut niveau dans le tableau de bord de Permissions Management
- Plongez plus profondément avec l'onglet Analytics
- Développez une meilleure compréhension de votre environnement avec les rapports
- Analysez les données historiques avec l'onglet Audit
- Agissez sur vos découvertes avec l'onglet Remediation de Permissions Management
- Adoptez une approche plus proactive avec la surveillance continue
- Gérez l'accès à Microsoft Entra Permissions Management
- Mise en œuvre de l'ensemble des fonctionnalités