Administration des accès et de l'identité Microsoft

Durée: 4 Jours **Réf de cours: M-SC300**

Résumé:

Cette formation permet d'acquérir les compétences et connaissances nécessaires pour mettre en œuvre des solutions de gestion de l'identité basées sur Microsoft Azure AD et sur les technologies d'identité connectées. Cette formation comprend le contenu de l'identité pour Azure AD, l'enregistrement des applications d'entreprise, l'accès conditionnel, la gouvernance des identités et d'autres outils d'identité.
Mise à jour : 08.02.2024

Public visé:

Cette formation s'adresse aux administrateurs d'identité et d'accès qui prévoient de passer l'examen de certification associé, ou qui effectuent des tâches d'administration d'identité et d'accès dans leur travail quotidien. Elle peut également être utile à un administrateur ou à un ingénieur qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion des accès pour les solutions basées sur Azure, jouant ainsi un rôle essentiel dans la protection d'une organisation.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Mettre en œuvre une solution de gestion des identités
- Mettre en œuvre une solution d'authentification et de gestion des accès
- Mettre en place une gestion des accès pour les applications
- Planifier et mettre en œuvre une stratégie de gouvernance des identités

Pré-requis:

Les stagiaires qui auront réussi auront une connaissance préalable et une compréhension des éléments suivants :

- Les meilleures pratiques de sécurité et les exigences de sécurité de l'industrie telles que la défense en profondeur, l'accès le moins privilégié, la responsabilité partagée et le modèle de confiance zéro.
- Connaître les concepts d'identité tels que l'authentification, l'autorisation et l'annuaire actif.
- Avoir une certaine expérience du déploiement de charges de travail Azure. Ce cours ne couvre pas les bases de l'administration d'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. Les laboratoires du cours peuvent utiliser PowerShell et le CLI.
- Cours préalables (ou connaissances équivalentes et expérience pratique) :

Cette formation en ligne gratuite vous permettra d'acquérir l'expérience nécessaire pour réussir ce cours.

- SC-900 partie 1 : Décrire les concepts de sécurité, de conformité et d'identité - Apprendre | Microsoft Docs
- SC-900 partie 2 : Décrire les capacités des solutions de gestion des identités et des accès de Microsoft - Apprendre | Microsoft Docs

- SC-900 partie 3 : Décrire les capacités des solutions de sécurité de Microsoft - Apprendre | Microsoft Docs
- SC-900 partie 4 : Décrire les capacités des solutions de conformité de Microsoft - Apprendre | Microsoft Docs
- AZ-104 : Gérer les identités et la gouvernance dans Azure - Apprendre | Microsoft Docs

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- M-SC100 - Microsoft Cybersecurity Architect

Contenu:

Mettre en œuvre une solution de gestion des identités

- Mettre en œuvre la configuration initiale d'Azure AD
- Créer, configurer et gérer les identités
- Mettre en œuvre et gérer les identités externes
- Implémenter et gérer les identités hybrides
- Lab 1a : Gérer les rôles des utilisateurs
- Lab 1b : Définir les propriétés des locataires
- Lab 1c : Attribuer des licences aux utilisateurs
- Lab 1d : Restaurer ou supprimer des utilisateurs supprimés
- Lab 1e : Ajouter des groupes dans Azure AD
- Lab 1f : Modifier les attributions de licences de groupe
- Lab 1g : Modifier les attributions de licences d'utilisateurs
- Lab 1h : Configurer la collaboration externe
- Lab 1i : Ajouter des utilisateurs invités à l'annuaire
- Lab 1j : Explorer les groupes dynamiques

Mettre en œuvre une solution d'authentification et de gestion des accès

- Sécuriser les utilisateurs Azure AD avec MFA
- Gérer l'authentification des utilisateurs
- Planifier, implémenter et administrer l'accès conditionnel
- Gérer la protection des identités Azure AD
- Lab 2a : Activer Azure AD MFA
- Lab 2b : Configurer et déployer la réinitialisation du mot de passe en libre-service (SSPR)
- Lab 2c : Travailler avec les paramètres de sécurité par défaut
- Lab 2d : Mettre en œuvre des politiques d'accès conditionnel, des rôles et des affectations
- Lab 2e : Configurer les contrôles de session d'authentification
- Lab 2f : Gérer les valeurs de verrouillage intelligent d'Azure AD
- Lab 2g : Activer la politique de risque de connexion
- Lab 2h : Configurer la politique d'enregistrement de l'authentification MFA d'Azure AD

Mettre en œuvre la gestion de l'accès aux applications

- Planifier et concevoir l'intégration de l'entreprise pour le SSO
- Mettre en œuvre et contrôler l'intégration des applications d'entreprise pour le SSO
- Implémenter l'enregistrement des applications
- Labo 3a : Implémenter la gestion des accès pour les applications
- Lab 3b : Créer un rôle personnalisé pour gérer l'enregistrement des applications
- Lab 3c : Enregistrer une application
- Lab 3d : Accorder le consentement de l'administrateur à l'ensemble du locataire pour une application
- Lab 3e : Ajouter des rôles aux applications et recevoir des jetons

Planifier et mettre en œuvre une stratégie de gouvernance des identités

- Planifier et mettre en œuvre la gestion des droits
- Planifier, implémenter et gérer les révisions d'accès
- Planifier et mettre en œuvre l'accès privilégié
- Surveiller et maintenir Azure AD
- Labo 4a : Créer et gérer un catalogue de ressources avec les droits Azure AD
- Lab 4b : Ajouter un rapport d'acceptation des conditions d'utilisation
- Lab 4c : Gérer le cycle de vie des utilisateurs externes avec Azure AD identity governance
- Lab 4d : Créer des revues d'accès pour les groupes et les applications
- Lab 4e : Configurer PIM pour les rôles Azure AD
- Lab 4f : Attribuer un rôle Azure AD dans PIM
- Lab 4g : Attribuer des rôles de ressources Azure dans PIM
- Lab 4h : Connecter les données d'Azure AD à Azure Sentinel

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Accès fourni au contenu digital officiel Microsoft
Important
Microsoft a sécurisé ses offres de formation en ajoutant l'authentification multi-facteurs (MFA) pour accéder aux tenants de Microsoft 365 et Dynamics 365.
Pour accéder à certains TP, les stagiaires devront activer la MFA. Ils auront besoin d'un téléphone portable pour configurer et vérifier la MFA. Ils auront également besoin d'une application capable de générer des codes d'authentification. L'application suggérée est Microsoft Mobile Phone Authenticator, qui est gratuite.
Voici le lien de téléchargement de l'application ainsi que la procédure d'installation :
Download the Microsoft Mobile Phone Authenticator App
Set up your Microsoft 365 sign-in for multi-factor authentication

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement