Security Operations Analyst Associate Microsoft

RS :

L'administrateur d'identité et d'accès Microsoft conçoit, implémente et exploite les systèmes de gestion des identités et des accès d'une organisation à l'aide d'Azure Active Directory (Azure AD)

Ce cours est destiné aux administrateurs d'identité et d'accès qui prévoient de passer l'examen de certification associé ou qui effectuent des tâches d'administration des identités et de l'accès dans le cadre de leur travail quotidien. Ce cours est également utile aux administrateurs ou aux ingénieurs qui souhaitent se spécialiser dans les solutions d'identité et les systèmes de gestion des accès pour les solutions basées sur Azure, et qui jouent un rôle essentiel dans la protection d'une organisation.

Programme

Mettre en œuvre une solution de gestion des identités

Implémenter la configuration initiale d'Azure Active Directory

- Configurer et gérer les rôles d'annuaire Azure AD
- Configurer et gérer des domaines personnalisés
- Configurer et gérer les options d'enregistrement des appareils
- Configurer la délégation à l'aide d'unités d'administration
- Configurer les paramètres à l'échelle du client

Créer, configurer et gérer des identités

- Créer, configurer et gérer des utilisateurs
- Créer, configurer et gérer des groupes
- Gérer des licences

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 (sociaux et SAML/WS-fed)

Implémenter et gérer l'identité hybride

- Implémenter et gérer Azure Active Directory Connect (AADC)
- Implémenter et gérer la synchronisation cloud Azure AD Connect
- Implémenter et gérer la synchronisation par hachage de mot de passe (PHS)
- Implémenter et gérer l'authentification directe (PTA)
- Mettre en œuvre et gérer l'authentification unique (SSO) transparente
- Implémenter et gérer la fédération (à l'exclusion des déploiements ADFS manuels)
- Implémenter et gérer Azure Active Directory Connect Health
- Résoudre les erreurs de synchronisation

Microsoft

Microsoft CERTIFIED
SECURITY OPERATIONS ANALYST
ASSOCIATE

LE PUBLIC VISÉ :
- Administrateur

DURÉE :
- 4 jours soit en total 28 heures

NIVEAU :
- Intermédiaire

TARIF :
- 2900€/personne

ELIGIBLE CPF :
- NON

Administration Sécurité Microsoft 365 (SC300)

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

Planifier et implémenter Azure Multifactor Authentication (MFA)

- Planifier le déploiement d'Azure MFA (à l'exclusion de MFA Server)
- Implémenter et gérer les paramètres Azure MFA
- Gérer les paramètres MFA pour les utilisateurs

Gérer l'authentification des 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 de mot de passe en libre-service
- Déployer et gérer la protection par mot de passe
- Configurer les seuils de verrouillage intelligent
- Mettre en œuvre et gérer les restrictions relatives aux locataires
- Planifier, mettre en œuvre et administrer l'accès conditionnel
- Planifier et mettre en œuvre des valeurs par défaut de sécurité
- Planifier des stratégies d'accès conditionnel
- Mettre en œuvre des contrôles et des affectations de stratégie d'accès conditionnel (ciblage, applications et conditions)
- Tester et dépanner des stratégies d'accès conditionnel
- Mettre en œuvre des contrôles d'application
- Mettre en œuvre la gestion des sessions

Gérer Azure AD Identity Protection

- Mettre en œuvre et gérer une politique de risque utilisateur
- Mettre en œuvre et gérer les politiques de risque
- Mettre en œuvre et gérer la politique d'enregistrement MFA
- Surveiller, enquêter et remédier aux utilisateurs à risque élevé

Mettre en œuvre la gestion des accès pour les applications

Planifier, mettre en œuvre et surveiller l'intégration des applications d'entreprise pour l'authentification unique

- Implémenter et configurer les paramètres de consentement
- Découvrir des applications à l'aide du rapport d'application MCAS ou ADFS
- Concevoir et mettre en œuvre la gestion des accès pour les applications
- Concevoir et implémenter des rôles de gestion d'applications
- Surveiller et auditer l'accès / Sign-iOns aux applications d'entreprise intégrées Azure Active Directory
- Intégrer des applications locales à l'aide du proxy d'application Azure AD
- Intégrer des applications SaaS personnalisées pour l'authentification unique
- Configurer des applications SaaS pré-intégrées (galerie)
- Implémenter l'approvisionnement des utilisateurs d'application

Implémenter les inscriptions d'applications

- Planifier votre stratégie d'enregistrement des applications métier
- Mettre en œuvre les enregistrements d'applications
- Configurer les autorisations d'application
- Mettre en œuvre l'autorisation de l'application
- Planifier et configurer des autorisations d'application multiples

Planifier et mettre en œuvre une stratégie de gouvernance des identités

Planifier et mettre en œuvre la gestion des droits

- Définir des catalogues
- Définir des packages d'accès
- Planifier, mettre en œuvre et gérer les droits
- Mettre en œuvre et gérer les conditions d'utilisation
- Gérer le cycle de vie des utilisateurs externes dans les paramètres azure ad identity governance

Administration Sécurité Microsoft 365 (SC300)

Planifier, mettre en œuvre et gérer les examens d'accès

- Planifier les examens d'accès
- Créer des avis d'accès pour les groupes et les applications
- Surveiller les résultats de l'examen de l'accès
- Gérer les licences pour les révisions d'accès
- Automatiser les tâches de gestion de la révision des accès
- Configurer les révisions d'accès récurrent

Planifier et mettre en œuvre l'accès privilégié

- Définir une stratégie d'accès privilégié pour les utilisateurs administratifs (ressources, rôles, approbations, seuils)
- Configurer la gestion des identités pour les rôles Azure AD
- Configurer la gestion des identités privilégiées pour les ressources Azure
- Attribuer des rôles
- Gérer les demandes PIM
- Analyser l'historique et les rapports d'audit PIM
- Créer et gérer des comptes bris de verre

Surveiller et gérer Azure Active Directory

- Analyser et examiner les journaux de connexion pour résoudre les problèmes d'accès
- Examiner et surveiller les journaux d'audit Azure AD
- Activer et intégrer les journaux de diagnostic Azure AD avec Log Analytics / Azure Sentinel
- Exporter les journaux de connexion et d'audit vers un SIEM tiers
- Examiner l'activité Azure AD à l'aide de Log Analytics / Azure Sentinel, à l'exclusion de l'utilisation de KQL
- Analyser les classeurs /rapports Azure Active Directory
- Configurer les notifications

Objectifs pédagogiques

Les administrateurs de l'identité et de l'accés gèrent des tâches telles que la fourniture d'une authentification sécurisée et d'un accès d'autorisation aux applications d'entreprise. L'administrateur fournit des expériences transparentes et des fonctionnalités de gestion en libre-service pour tous les utilisateurs. L'accès adaptatif et la gouvernance sont des éléments essentiels du rôle. Ce rôle est également responsable du dépannage, de la surveillance et de la création de rapports pour l'environnement d'identité et d'accès.
L'administrateur d'identité et d'accès peut être une seule personne ou un membre d'une équipe plus importante. Ce rôle collabore avec de nombreux autres rôles de l'organisation pour mener des projets d'identité stratégiques afin de moderniser les solutions d'identité, de mettre en œuvre des solutions d'identité hybrides et de mettre en œuvre la gouvernance des identités

A l'issu de l'examen le candidat sera en mesure de :

- Mettre en œuvre une solution de gestion des identités.
- Mettre en œuvre une solution d'authentification et de gestion des accès.
- Implémentez la gestion des accès pour les applications.
- Planifier et mettre en œuvre une stratégie de gouvernance des identités.

Méthode et 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 en français sera remis aux participants au format électronique via la plateforme

Evaluation :
les acquis sont évalués tout au long de la formation et en fin de formation par le formateur (questions régulières, travaux pratiques, QCM ou autres méthodes).

Formateur :
le tout animé par un consultant-formateur expérimenté, nourri d'une expérience terrain, et accrédité Microsoft Certified Trainer.

Administration Sécurité Microsoft 365 (SC300)

Méthode et modalités pédagogiques

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. Les appréciations que vous avez formulées font l'objet d'un enregistrement et d'une analyse qualitative de la formation et du formateur. ITsystème formation dispose d'un processus qualité qui prend en considération les retours des participants afin d'être proactif quant à la solution corrective adaptée.
Nous veillons à ce que tous les objectifs de l'examen soient couverts en profondeur afin que vous soyez prêt pour toute question de l'examen. Nos tests pratiques sont rédigés par des experts de l'industrie en la matière. Ils travaillent en étroite collaboration avec les fournisseurs de certification pour comprendre les objectifs de l'examen, participer aux tests bêta et passer l'examen eux-mêmes avant de créer de nouveaux tests pratiques.

Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
Les simulations en ligne basées sur la performance offrent une expérience pratique de l'environnement de travail
Les questions sont similaires aux questions d'examen afin que vous testiez votre connaissance des objectifs de l'examen
Des explications détaillées pour les réponses correctes et distractrices renforcent le matériel
Le mode étude couvre tous les objectifs en veillant à ce que les sujets soient couverts
Le mode de certification (chronométré) prépare les étudiants aux conditions de passage des examens
Des rapports de score instantanés et approfondis vous indiquent exactement les domaines sur lesquels vous concentrer.
Cette formation peut être dispensée en mode présentiel comme en distanciel.
Elle prend en charge les compétences ci-dessous ; le pourcentage indique le poids relatif du module dans l'examen global. Plus vous vous concentrez sur des modules avec un pourcentage plus élevé, plus vous obtiendrez probablement plus de notes à l'examen.

Cet examen mesure votre capacité à accomplir les tâches techniques suivantes :

- Mettre en œuvre une solution de gestion des identités (25-30%)
- Mettre en œuvre une solution d'authentification et de gestion des accès (25-30 %)
- Mettre en œuvre la gestion des accès pour les applications (10 à 15 %)
- Planifier et mettre en œuvre une stratégie de gouvernance des identités (25 à 30 %)

Pour qui ?

Ce cours est destiné aux administrateurs d'identité et d'accès qui prévoient de passer l'examen de certification associé ou qui effectuent des tâches d'administration des identités et de l'accès dans le cadre de leur travail quotidien. Ce cours est également utile aux administrateurs ou aux ingénieurs qui souhaitent se spécialiser dans les solutions d'identité et les systèmes de gestion des accès pour les solutions basées sur Azure, et qui jouent un rôle essentiel dans la protection d'une organisation.

Pré-requis

• Meilleures pratiques de sécurité et exigences de sécurité du secteur telles que la défense en profondeur, l'accès le moins privilégié, la responsabilité partagée et le modèle zero trust.
• Se familiariser avec les concepts d'identité tels que l'authentification, l'autorisation et Active Directory.
• Avoir de l'expérience dans le déploiement de charges de travail Azure. Cette formation ne couvre pas les bases de l'administration Azure, mais elle s'appuie sur ces connaissances en ajoutant des informations spécifiques à la sécurité.
• Une certaine expérience avec les systèmes d'exploitation Windows et Linux et les langages de script est utile mais pas obligatoire. Les laboratoires de cours peuvent utiliser PowerShell et l'interface de ligne de commande.
• Cours préalables SC 900 & AZ 104 ou connaissances équivalentes et expérience pratique

Accessibilité

Il est possible de vous inscrire jusqu'à 2 jours ouvrés avant le début de la formation, sous condition de places disponibles et de réception du devis signé.
Il est aussi possible – sur demande – d'adapter des moyens de la prestation pour les personnes en situation de handicap en fonction du type de handicap.
Le centre de formation ITsystem Formation est situé au :
Grand Paris au
21 rue jean Rostand
91898 ORSAY

Vous pouvez facilement y accéder par les transports en commun suivants :
RER B Le guichet BUS 11 et BUS 7
En voiture : prendre la N118, sortie 9 Centre universitaire Grandes écoles

Pré certification

Cette formation ouvre la voie à la « **certification SC-300 Administrateur de l'identité et de l'accès Microsoft »**