REFERENTIEL DE COMPETENCES ET D'EVALUATION DE LA CERTIFICATION

Administrer la sécurité des postes de travail Microsoft 365

(titre en anglais : Microsoft 365 Certified: Security Administrator Associate)

MODALITES D'EVALUATION

Pour obtenir cette certification, il est proposé au candidat d'évaluer leurs compétences à travers un (1) examen en ligne, supervisé par l'organisme Pearson VUE, délivré dans un centre d'examen accrédité (ou via de la surveillance à distance).

L'examen dure environ deux (2) heures – livres fermés - et comprend une variété de questions appelant différentes formes de réponse* : Écran actif, Meilleure réponse, Construction de liste, Études de cas, Glisser-déplacer, Zone réactive, Choix multiple, Plusieurs choix de réponse, Réponse courte, Révision des notes, Écran de révision.
*Détaillées à cette URL : https://www.microsoft.com/en-us/learning/certification-exams.aspx?types=true

Le seuil de réussite est fixé à environ 70% de bonnes réponses, qui correspond à un score de passage de 700 points (score à l'échelle). Le pourcentage réel varie d'un examen à l'autre. La note de passage est basée sur l'apport d'experts en la matière, le niveau de compétence requis pour être considéré comme compétent dans le domaine du contenu, et la difficulté des questions livrées pendant l'examen. Les pourcentages dans le tableau des compétences évaluées indiquent le poids relatif de chaque sujet principal de l'examen. Plus le pourcentage est élevé, plus les candidats devront répondre à des questions sur cette zone de contenu. La liste des tâches évaluées n'est pas exhaustive et peut couvrir d'autres tâches dans le cadre des compétences évaluées.

Le contenu des tests est réévalué régulièrement par les équipes Microsoft, soit en termes de corrections d'expression, soit vis-à-vis des fonctionnalités de sécurité ou de types de questions (dernière mise à jour de cet examen le 27 janvier 2021).

COMPETENCES GENERALES :

Les candidats à cet examen sont des administrateurs système ou spécialistes qui mettent en oeuvre, gèrent et surveillent les solutions de sécurité et de conformité pour les postes de travail Microsoft 365 et les environnements hybrides. Une fois certifiés, les professionnels sécuriseront de manière proactive les environnements de Microsoft 365 Entreprise pour répondre aux menaces, mener des enquêtes et appliquer la gouvernance des données. Les détenteurs de la certification « administrer la sécurité pour Microsoft 365 » collaborent avec l'administrateur système principal, le cas échéant, mais aussi avec les parties prenantes de l'entreprise, et d'autres administrateurs de charges de travail pour planifier et mettre en œuvre les stratégies de sécurité et s'assurer que les solutions sont conformes aux politiques et réglementations de l'organisation.

Les candidats à cet examen sont familiarisés aux charges de travail de Microsoft 365 et possèdent des compétences solides et de l'expérience dans la protection de l'identité, la protection des informations, la protection contre les menaces, la gestion de la sécurité et la gouvernance des données. Ce rôle se concentre sur l'environnement Microsoft 365 et comprend des environnements hybrides.

L'examen de certification mesure la capacité des candidats à déployer les compétences techniques suivantes (détaillées ensuite par tâches ci-dessous) : implémenter et gérer les identités et les accès, implémenter et gérer la protection contre les menaces, implémenter et gérer la protection des informations et gérer les options de gouvernance et de conformité dans Microsoft 365.

COMPETENCES MOBILISABLES EVALUEES		**Nature des tâches qui constituent la compétence**	**EVALUATION**		
Sur 100% :			**% de l'évaluation globale**	**Modalités d'évaluation**	**Critères**
Implémenter et gérer les identités et les accès			**30-35% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 40 minutes** (pour 18 à 20 questions) sont consacrées à cette compétence	Le taux de bonnes réponses doit être au global de **70% minimum**
	Sécuriser les environnements hybrides avec Microsoft 365	• planifier les options d'authentification Azure AD • planifier les options de synchronisation Azure AD • surveiller et dépanner les événements Azure AD Connect			
	Sécuriser les identités	• implémenter l'appartenance au groupe Azure AD • implémenter la gestion des mots de passe • configurer et gérer la gouvernance des identités			
	Mettre en œuvre des méthodes d'authentification	• planifier la sécurité de la connexion • implémenter l'authentification multifacteurs (MFA) • gérer et surveiller la MFA • planifier et mettre en œuvre des méthodes d'authentification d'appareil comme Windows Hello • configurer et gérer les options d'authentification des utilisateurs Azure AD et la gestion des mots de passe en libre-service			

	Mettre en œuvre un accès conditionnel	• planifier les politiques de conformité et d'accès conditionnel • configurer et gérer la conformité des appareils pour la sécurité des terminaux • implémenter et gérer l'accès conditionnel			
	Implémenter le contrôle d'accès basé sur les rôles (RBAC) pour assurer une gestion précise de l'accès aux ressources Azure	• planifier les rôles • configurer les rôles • Auditer les rôles			
	Mettre en œuvre Azure AD Privileged Identity Management (PIM) pour gérer et superviser l'accès aux ressources importantes de l'organisation	• planifier Azure PIM • attribuer l'éligibilité et activer les rôles d'administrateur • gérer les demandes et attributions de rôles Azure PIM • surveiller l'historique et les alertes PIM			
	Mettre en œuvre la protection d'identité Azure AD	• mettre en œuvre une politique de risque utilisateur • mettre en œuvre une politique de risque de connexion • configurer les alertes de protection d'identité • examiner les événements à risque et y répondre			
Implémenter et gérer la protection contre les menaces			**20-25% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 30 minutes** (pour 12 à 14 questions)	Le taux de bonnes réponses doit être au global de 70% minimum
	Mettre en œuvre une solution de protection hybride contre les menaces d'entreprise	• planifier une solution Microsoft Defender for Identity • installer et configurer Microsoft Defender pour l'identité • surveiller et gérer Microsoft Defender pour l'identité			
	Mettre en œuvre une protection contre les menaces des appareils (ou terminaux)	• planifier une solution Microsoft Defender pour les terminaux • implémenter Microsoft Defender pour les terminaux • gérer et surveiller Microsoft Defender pour les terminaux			

	Mettre en œuvre et gérer la protection des appareils et des applications	• planifier la protection des appareils et des applications • configurer et gérer Microsoft Defender Application Guard • configurer et gérer Microsoft Defender Application Control • configurer et gérer la protection contre les exploits • configurer le démarrage sécurisé • configurer et gérer le chiffrement des appareils Windows et non Windows • planifier la sécurisation des données des applications sur les appareils • mettre en œuvre des politiques de protection des applications		sont consacrées à cette compétence	
	Mettre en œuvre et gérer le composant antivirus Microsoft Defender pour Office 365	• configurer Microsoft Defender pour Office 365 • surveiller Microsoft Defender pour Office 365 • mener des attaques simulées à l'aide du simulateur d'attaque			
	Surveiller la sécurité de Microsoft 365 avec Azure Sentinel, outil de SIEM (Security Information and Event Management)	• planifier et mettre en œuvre Azure Sentinel • configurer des playbooks dans Azure Sentinel • gérer et surveiller Azure Sentinel • répondre aux menaces dans Azure Sentinel			
Implémenter et gérer la protection des informations			**15-20% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 20 minutes** (pour 10-12 questions)	Le taux de bonnes réponses doit être au global de 70% minimum
	Sécuriser l'accès aux données dans Office 365	• implémenter et gérer le Customer Lockbox • configurer l'accès aux données dans les charges de travail de collaboration Office 365 • configurer le partage B2B pour les utilisateurs externes			
	Gérer les étiquettes de sensibilité	• planifier une solution d'étiquette de sensibilité • configurer les étiquettes et les politiques de sensibilité • configurer et utiliser l'analyse des étiquettes • utiliser des étiquettes de sensibilité avec les applications Teams, Sharepoint, OneDrive et Office			

	Gérer la prévention de la perte de données (DLP)	• planifier une solution DLP • créer et gérer les politiques DLP • créer et gérer des types d'informations sensibles • surveiller les rapports DLP et gérer les notifications		sont consacrées à cette compétence	
	Mettre en œuvre et gérer la sécurité des applications Microsoft Cloud	• planifier la mise en œuvre de Cloud App Security • configurer la sécurité des applications Microsoft Cloud • gérer la découverte d'applications cloud • gérer les entrées dans le catalogue d'applications Cloud • gérer les applications dans Cloud App Security • gérer la sécurité des applications Microsoft Cloud • configurer les connecteurs Cloud App Security et les applications Oauth • configurer les politiques et les modèles de sécurité des applications cloud • examiner, interpréter et répondre aux alertes, rapports, tableaux de bord et journaux de Cloud App Security			
Gérer les options de gouvernance et de conformité dans Microsoft 365			**20-25% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 30 minutes** (pour 12 à 14 questions) sont consacrées à cette compétence	Le taux de bonnes réponses doit être au global de 70% minimum
	Configurer et analyser les rapports de sécurité	• surveiller et gérer l'état de sécurité de l'appareil à l'aide de la console d'administration Microsoft Endpoint Manager Admin Center • gérer et surveiller la sécurité et les tableaux de bord à l'aide de Microsoft 365 Security Center • planifier des rapports de sécurité personnalisés avec l'API Graph Security • utiliser des tableaux de bord de score sécurisés pour examiner les actions et les recommandations • configurer les stratégies d'alerte dans le centre de sécurité Microsoft 365			
	Gérer et analyser les journaux et rapports d'audit	• planifier l'audit et le reporting • effectuer une recherche dans le journal d'audit • examiner et interpréter les rapports de conformité et les tableaux de bord			

		• configurer la stratégie d'alerte d'audit			
	Gérer la gouvernance et la conservation des données	• planifier la gouvernance et la conservation des données • examiner et interpréter les rapports et tableaux de bord de gouvernance des données • configurer les étiquettes et les politiques de rétention • définir les types d'événements de gouvernance des données • définir et gérer les politiques de conformité des communications • configurer les conservations d'informations • rechercher et récupérer des données Office 365 supprimées • configurer l'archivage des données • gérer les boîtes aux lettres inactives			
	Gérer la recherche et l'enquête	• planifier la recherche de contenu et la découverte électronique • déléguer les autorisations pour utiliser les outils de recherche et de découverte • utiliser des outils de recherche et d'enquête pour effectuer des recherches de contenu • exporter les résultats de la recherche de contenu • gérer les cas d'eDiscovery			
	Gérer la conformité à la réglementation sur la confidentialité des données	• planifier la conformité réglementaire dans Microsoft 365 • examiner et interpréter les tableaux de bord et rapports GDPR • gérer les demandes des personnes concernées (DSR) • administrer le Compliance Manager • examiner les rapports du Compliance Manager • créer et réaliser des évaluations et des actions de Compliance Manager			