REFERENTIEL DE COMPETENCES ET D'EVALUATION DE LA CERTIFICATION

GARANTIR LA SECURITE DE L'INFRASTRUCTURE CLOUD MICROSOFT AZURE

(titre en anglais : Microsoft Certified Azure Security Engineer 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 (dernière mise à jour le 24 septembre 2020).

COMPETENCES GENERALES :

Les candidats à l'examen Azure sécurité sont des ingénieurs de sécurité spécialisés pour le Cloud Microsoft Azure, qui mettent en œuvre des contrôles de sécurité, maintiennent la posture de sécurité, gèrent l'identité et l'accès et protègent les données, les applications et les réseaux. Les candidats identifient et corrigent les vulnérabilités à l'aide d'une variété d'outils de sécurité, mettent en œuvre une protection contre les menaces et répondent aux escalades d'incidents de sécurité. En tant qu'ingénieur de sécurité Microsoft Azure, les candidats font souvent partie d'une équipe plus grande dédiée à la gestion et à la sécurité basées sur le cloud et peuvent également sécuriser des environnements hybrides dans le cadre d'une infrastructure de bout en bout.

Les candidats à cet examen doivent avoir de solides compétences en écriture de scripts et en automatisation, une connaissance approfondie des réseaux, de la virtualisation et de l'architecture cloud à N niveaux, ainsi qu'une solide connaissance des capacités du cloud, des produits et services Microsoft Azure et d'autres produits et services Microsoft.

Microsoft

L’examen de certification mesure la capacité des candidats à déployer les compétences techniques suivantes (détaillées ensuite par tâches ci-dessous) : gérer l'identité et l'accès pour les utilisateurs, mettre en œuvre la protection de la plateforme, gérer les opérations de sécurité et sécuriser les données et les applications de l’entreprise.

COMPETENCES MOBILISABLES EVALUEES		**Nature des tâches qui constituent la compétence**	**EVALUATION**		
Sur 100% :			**% de l’évaluation globale**	**Modalités d’évaluation**	**Critères**
Gérer l'identité et l'accès des utilisateurs aux applications et données selon les besoins			**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**
	Configurer l’annuaire Azure Active Directory pour organiser les charges de travail	• créer l'enregistrement d'application • configurer les étendues de permission d'enregistrement d'application • gérer le consentement de l'autorisation d'enregistrement d'application • configurer les paramètres d'authentification multifacteur • gérer les groupes d'annuaires Azure AD • gérer les utilisateurs Azure AD • installer et configurer Azure AD Connect • configurer les méthodes d'authentification • mettre en œuvre des politiques d'accès conditionnel • configurer la protection d'identité Azure AD			
	Configurer la console de gestion Azure AD Privileged Identity Management	• surveiller l'accès privilégié • configurer les revues d’accès • activer la gestion des identités privilégiées			
	Configurer la sécurité des locataires Azure	• transférer des abonnements Azure entre des locataires Azure AD • gérer l'accès API aux abonnements et ressources Azure			

Mettre en œuvre la protection de la plateforme contre les accès indésirables			**15-20% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 20 minutes** (pour 10 à 12 questions) sont consacrées à cette compétence	Le taux de bonnes réponses doit être au global de 70% minimum
	Mettre en œuvre la sécurité du réseau	• configurer la connectivité du réseau virtuel • configurer les groupes de sécurité réseau (NSG) • créer et configurer le Firewall Azure • créer et configurer le service Azure Front Door • créer et configurer des groupes de sécurité d'application • configurer la gestion des accès à distance • configurer la ligne de base • configurer le pare-feu des ressources			
	Mettre en œuvre la sécurité de l'hôte	• configurer la sécurité des terminaux au sein de la machine virtuelle • configurer la sécurité des VM • renforcer l'utilisation des machines virtuelles dans Azure • configurer les mises à jour système pour les machines virtuelles dans Azure • configurer la ligne de base			
	Configurer la sécurité des conteneurs	• configurer le réseau • configurer l'authentification • configurer l'isolement des conteneurs • configurer la sécurité AKS • configurer le registre des conteneurs • implémenter la gestion des vulnérabilités			
	Mettre en œuvre la sécurité de la gestion des ressources Azure	• créer des verrous de ressources Azure • gérer la sécurité des groupes de ressources • configurer les stratégies Azure • configurer des rôles RBAC personnalisés • configurer les autorisations d'abonnement et de ressources			

Gérer les opérations de sécurité au quotidien pour surveiller et anticiper toute alerte malveillante			**25-30% de l'évaluation globale**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 35 minutes** (pour 14-16 questions) sont consacrées à cette compétence	Le taux de bonnes réponses doit être au global de 70% minimum
	Configurer les services de sécurité	• configurer Azure Monitor • configurer la journalisation des diagnostics et la conservation des journaux • configurer l'analyse des vulnérabilités			
	Configurer les politiques de sécurité	• configurer la gestion centralisée des stratégies à l'aide d'Azure Security Center • configurer l'accès aux machines virtuelles juste à temps à l'aide d'Azure Security Center			
	Gérer les alertes de sécurité	• créer et personnaliser des alertes • examiner et répondre aux alertes et recommandations • configurer un playbook pour un événement de sécurité à l'aide d'Azure Security Center • enquêter sur les incidents de sécurité aggravés			
Sécuriser les données et les applications, en gérant le stockage, la sauvegarde et leurs accès			**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	Le taux de bonnes réponses doit être au global de 70% minimum
	Configurer des politiques de sécurité pour gérer les données	• configurer la classification des données • configurer la conservation des données • configurer la souveraineté des données			
	Configurer la sécurité de l'infrastructure de données	• activer l'authentification de la base de données • activer l'audit de la base de données • configurer la protection avancée contre les menaces pour la base de données Azure SQL • configurer le contrôle d'accès et la gestion des clés pour les comptes de stockage • configurer l'authentification Azure AD pour Azure Storage			

		• configurer l'authentification des services de domaine Azure AD pour les fichiers Azure • créer et gérer des signatures d'accès partagé (SAS) • configurer la sécurité pour HDInsights, Cosmos DB et pour Azure Data Lake		cette compétence	
	Configurer le chiffrement des données au bon moment	• implémenter Azure SQL Database Always Encrypted • implémenter le chiffrement de la base de données • implémenter le chiffrement du service de stockage • implémenter le chiffrement du disque			
	Configurer la sécurité des applications	• configurer les certificats SSL / TLS • configurer les services Azure pour protéger les applications Web • créer une ligne de base de sécurité des applications			
	Configurer et gérer Key Vault pour chiffrer des clés et des mots de passe	• gérer l'accès à Key Vault • gérer les autorisations avec les mots de passe, les certificats et les clés • configurer l'utilisation de RBAC dans Azure Key Vault • gérer les certificats • configurer la rotation des clés			