REFERENTIEL D'EVALUATION ET DE COMPETENCES DE LA CERTIFICATION

GARANTIR LA SECURITE DU CLOUD AWS

(Titre en anglais : AWS Certified Security – Specialty)

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 ou PSI Services, délivrés dans un centre d'examen accrédité (ou via de la surveillance à distance).

L'examen dure environ deux heures et cinquante minutes (2h50) – livres fermés - et comprend une variété de questions appelant différentes formes de réponse* : Questions à choix multiples, Questions à réponses multiples.
*Détaillées à cette URL : https://d1.awsstatic.com/training-and-certification/docs-security-spec/AWS-Certified-Security-Specialty_Exam-Guide.pdf

Le seuil de réussite est fixé à environ 75% de bonnes réponses, qui correspond à un score de passage de 750 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.

L'examen compte en tout 65 questions mais seulement 50 sont évaluées. L'examen comprend 15 questions non notées qui n'affectent pas le score du candidat. AWS collecte des informations sur la performance des candidats sur ces questions non notées afin d'évaluer ces questions en vue d'une utilisation future. Ces questions non notées ne sont pas identifiées lors de l'examen. Dans le résumé des compétences ci-dessous le pourcentage représente uniquement le contenu scoré. Il en est de même pour le nombre de questions par domaine évalué.

Le contenu des tests est réévalué régulièrement par les équipes Amazon Web Services pour refléter les dernières évolutions des services et de la plate-forme AWS.

RESUME DES ACTIVITES PRINCIPALES :

Compétences mobilisables évaluées		Nature des tâches évaluées permettant de valider la compétence	Evaluation		
			% de l'évaluation globale	**Modalités d'évaluation**	**Critères**
Repérer, évaluer et répondre aux incidents de sécurité compromettant l'intégrité de votre infrastructure cloud			**12% de l'évaluation globale de l'examen**	Examen en ligne avec une variété de questions (cf. détail plus haut) ** **Environ 21 minutes** (pour 6 à 8 questions évaluées) sont consacrées à cette compétence	Examen compensatoire, le taux de bonnes réponses doit être au **global** de **75% minimum**
	Compte tenu d'un avis d'abus AWS, évaluer l'instance suspectée comme compromise ou les clés d'accès exposées.	▸ Compte tenu d'un report d'abus AWS, isoler les ressources affectées par l'incident en vue d'une investigation légale. ▸ S'assurer d'avoir les logs, snapshots et autres données nécessaires pour mener à bien l'enquête sur l'incident, pour une analyse approfondie ultérieure ou pour des raisons de conformité légale. ▸ Analysez les journaux pertinents pour une instance signalée afin de vérifier une violation et de collecter des données pertinentes.			
	Vérifier que le plan de réponse aux incidents inclut les services AWS pertinents	▸ Déterminez si des modifications ont été apportées à la configuration de sécurité de base. ▸ Déterminez si la liste omet les services, processus ou procédures qui facilitent la réponse aux incidents. ▸ Recommander des services, des processus et des procédures pour remédier aux lacunes. ▸ Automatiser les taches de routine à réaliser lors d'une réponse a un incident grave aux APIs (par exemple savoir en une ligne de commande isoler une instance grâce aux groupes de sécurité). ▸ Utiliser Forensics sur les volumes de données ainsi qu'utiliser les snapshots d'Amazon EBS pour capturer les données et l'état du système sous surveillance. ▸ Utiliser AWS CloudFormation pour déployer des instances préconfigurées dans un environnement isolé qui contient			

		tous les outils nécessaires pour déterminer la cause de l'incident. ▸ Utiliser AWS Step Functions pour déployer et utiliser des services tels que AWS Lambda et AWS CloudFormation pour répondre aux incidents dans le cloud.			
	Évaluer la configuration des alertes automatisées et procéder à une éventuelle correction des incidents liés à la sécurité et autres questions émergentes.	▸ S'assurer que les bonnes politiques IAM sont en place pour que l'équipe en charge de la réponse aient la permission « lecture seul ». ▸ Automatisez l'évaluation de la conformité à l'aide de règles pour les ressources nouvelles, modifiées/supprimées. ▸ Comprendre le fonctionnement des notifications d'abus générées par le bot et suivre le procédé établi en cas de compte AWS compromis. ▸ Passer en revue les incidents de sécurité précédents et recommander des améliorations aux systèmes existants.			
Enregistrer et surveiller les actions des différents acteurs utilisant le cloud AWS			**20% de l'évaluation globale de l'examen**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 35 minutes** (pour 9 à 11 questions évaluées) sont consacrées à cette compétence	Examen compensatoire, le taux de bonnes réponses doit être au **global** de **75% minimum**
	Concevoir et mettre en œuvre la surveillance de la sécurité et des alertes.	▸ Paramétrer un système de surveillance avec Amazon CloudWatch et programmer l'envoi d'alertes en créant des fonctions AWS Lambda et en paramétrant Amazon SNS. ▸ Paramétrer des agents Amazon CloudWatch pour avoir une surveillance par service utilisé. ▸ Enregistrer les changements de configuration du cloud avec AWS Config. ▸ Utiliser EC2 Intrusion Detection pour monitorer le réseau et les systèmes face à toutes activités malicieuses.			
	Résoudre les problèmes de surveillance et d'alerte de sécurité.	▸ Utiliser AWS Config pour monitorer, détecter et résoudre les problèmes de non-conformité en temps réel. ▸ Compte tenu de l'occurrence d'un événement connu sans l'alerte attendue, analyser la fonctionnalité et la configuration du service, puis corriger. ▸ Compte tenu de l'occurrence d'un événement connu sans l'alerte attendue, analyser les autorisations et corriger.			

		▸ Compte tenu d'une application personnalisée qui ne rapporte pas ses statistiques, analyser la configuration et corriger. ▸ Examiner les pistes d'audit de l'activité du système et des utilisateurs.			
	Concevoir et mettre en œuvre une solution d'enregistrement des actions / de journalisation.	▸ Utiliser les différents services permettant d'enregistrer les différentes actions des utilisateurs. En particulier savoir utiliser AWS CloudTrail pour enregistrer et traquer les différents changements sur les ressources AWS (création, modifications, suppression) ▸ Identifier les exigences de journalisation et les sources d'ingestion de journaux. Analyser les exigences et implémenter un stockage de journaux durable et sécurisé conformément aux meilleurs pratiques AWS. ▸ Utiliser la console de management AWS ou CLI pour accéder aux services suivants et regrouper les informations nécessaires à un audit : Amazon S3 Server Access logs, ELB Access logs, Amazon CloudWatch Logs and Events, Amazon VPC Flow logs, AWS CloudTrail. ▸ Tirer parti d'Amazon GuardDuty, AWS Trusted Advisor, AWS Security Hub pour enregistrer et surveiller les différentes APIs.			
	Résoudre les problèmes liés aux solutions d'enregistrement des actions.	▸ Consulter AWS Artifact pour accéder aux rapports de sécurité et de conformité. ▸ Accéder aux différentes ressources supports telles que les programmes de conformité AWS, le centre de conformité AWS, les workbooks sur les pratiques à privilégier, … ▸ Compte tenu de l'absence de journaux, déterminer la configuration incorrecte et définir les étapes de correction. ▸ Analyser les autorisations d'accès à la journalisation pour déterminer la configuration incorrecte et définir les étapes de correction.			

Créer et Implémenter la sécurité de l'infrastructure cloud AWS (périphérie et infrastructure réseau)			**26% de l'évaluation globale de l'examen**	Examen en ligne avec une variété de questions (cf détail plus haut) ** **Environ 45 minutes** (pour 12 à 14 questions évaluées) sont consacrées à cette compétence	Examen compensatoire, le taux de bonnes réponses doit être au **global** de **75% minimum**
	Concevoir une sécurité de périphérie sur AWS.	▸ Appliquer les différents concepts pour un cloud aussi sécurisé et conforme que possible : ○ Mettre en œuvre une solide base identitaire, ○ Activer la traçabilité, ○ Appliquer la sécurité a toutes les couches, ○ Automatiser les meilleures pratiques en matière de sécurité, ○ Protéger les données en transit et au repos, ○ Appliquer le principe du moindre privilège, ○ Préparer les évènements de sécurité, ○ Evaluer et limiter la surface d'attaque pour une charge de travail donnée, ○ Réduire le rayon d'explosion (par exemple en distribuant les applications entre les comptes et les régions) ▸ Maitriser le système de sécurité des centres de données AWS (couche environnementale, infrastructure, couche de la data). ▸ Choisir les services Edge AWS et/ou tiers appropriés tels que WAF, CloudFront et Route 53 pour vous protéger contre les attaques DDoS ou filtrer les attaques au niveau de l'application. ▸ Compte tenu d'un ensemble d'exigences de protection des bords pour une application, évaluer les mécanismes de prévention et de détection des intrusions à des fins de conformité et recommandez les modifications requises. ▸ Tester les règles WAF pour vous assurer qu'elles bloquent le trafic malveillant.			
	Concevoir et mettre en œuvre une infrastructure réseau sécurisée.	▸ Protéger une infrastructure réseau par isolation : subnet routing, listes de contrôle d'accès au réseau (NACLs), groupes de sécurité. ▸ Utiliser AWS Systems Manager pour automatiser certaines tâches de gestion (collection des informations du systèmes,			

		application de patches à l'OS, maintenance et mises à jour des antivirus, …). ▸ Utiliser AWS Firewall Manager pour configurer et gérer de manière centrale toutes les règles de firewall des différentes applications et du compte AWS. ▸ Configurer AWS Direct Connect pour établir et sécuriser une connexion entre des serveurs physiques et le cloud AWS. ▸ Utiliser AWS CloudFormation pour automatiser le déploiement des contrôles de sécurité et de conformité sur l'environnement AWS. ▸ Désactivez tous les ports et protocoles réseau inutiles. ▸ Compte tenu d'un ensemble d'exigences de protection Edge, évaluez la conformité des groupes de sécurité et des NACL d'une application et recommandez les modifications requises. ▸ Compte tenu des exigences de sécurité, décidez de la segmentation du réseau (par exemple les groupes de sécurité et les NACL) qui autorisent le minimum d'accès entrée/sortie requis. ▸ Compte tenu d'une description de l'infrastructure réseau d'un VPC, analysez l'utilisation de sous-réseaux et de passerelles pour un fonctionnement sécurisé.			
	Dépanner une infrastructure réseau sécurisée.	▸ Suivre les processus pour intervenir sur une infrastructure réseau sécurisé en panne/présentant des anomalies. ▸ Réaliser des tests de pénétration une fois le dépannage achevé sur EC2, EBS, Amazon RDS, Amazon Api Gateways. ▸ Mettre à profit les ressources proposées par AWS et le support associé au type de compte AWS pour aider au dépannage. ▸ Déterminer où le flux de trafic réseau est refusé. ▸ Compte tenu d'une configuration, vérifiez que les groupes de sécurité et les NACL ont été correctement implémentés.			

	Concevoir et mettre en œuvre la sécurité basée sur l'hôte.	▸ Utiliser Amazon Route 53 pour éviter toute panne de votre site internet et applications web hébergées sur AWS et pour protéger votre infrastructure de toute attaque DDoS. ▸ Utiliser Amazon Cloudfront pour protéger les transferts de données des attaques DDoS. ▸ Protéger les applications web avec AWS Shield et AWS Advanced Shield pour réduire la latence et le temps d'arrêt ainsi que pour prévenir en temps réel les attaques DDoS, jusqu'aux plus sophistiquées avec AWS Advanced Shield. ▸ Définir les règles sur le trafic entrant et sortant avec AWS Web Application Firewall (WAF) pour prévenir l'exploitation des faiblesses web pouvant compromettre la sécurité des applications ou surconsommer des ressources.			
Concevoir, mettre en œuvre et surveiller les règles de gestion des identités et des accès			**20% de l'évaluation globale de l'examen**	Examen en ligne avec une variété de questions (cf. détail plus haut) ** **Environ 35 minutes** (pour 9 à 11 questions évaluées) sont consacrées à cette compétence	Examen compensatoire, le taux de bonnes réponses doit être au **global** de **75% minimum**
	Concevoir et mettre en œuvre un système d'autorisation et d'authentification évolutif pour accéder aux ressources AWS.	▸ Compte tenu d'une description d'une charge de travail, analyser la configuration du contrôle d'accès pour les services AWS et formuler des recommandations qui réduisent les risques. ▸ Compte tenu d'une description de la façon dont une organisation gère ses comptes AWS, vérifiez la sécurité de son utilisateur racine. ▸ Compte tenu des exigences de conformité de votre organisation, déterminer quand appliquer des stratégies utilisateur et des stratégies de ressources. ▸ Dans la stratégie d'une organisation, déterminer quand fédérer un service d'annuaire à IAM. ▸ Concevoir un modèle d'autorisation évolutif qui inclut des utilisateurs, des groupes, des rôles et des stratégies. ▸ Identifier et limiter l'accès des utilisateurs individuels aux données et aux ressources AWS. ▸ Examinez les stratégies pour établir que les utilisateurs/systèmes ne peuvent pas exécuter des fonctions au-delà de leur responsabilité, et appliquent également une séparation appropriée des tâches.			

		▸ Créer des accès aux applications web et mobiles grâce aux réseaux sociaux en suivant le principe du moindre privilège avec Amazon Cognito.			
	Dépanner un système d'autorisation et d'authentification pour accéder aux ressources AWS.	▸ Étudier l'incapacité d'un utilisateur à accéder au contenu du compartiment S3. ▸ Étudier l'incapacité d'un utilisateur à basculer des rôles vers un autre compte. ▸ Étudier l'incapacité d'une instance Amazon EC2 à accéder à une ressource AWS donnée. ▸ Utiliser AWS Federated Identity avec le service de fédération Active Directory pour passer outre les problèmes de système d'autorisation. ▸ Mettre à profit les ressources proposées par AWS et le support associé au type de compte AWS pour aider au dépannage.			
Implémenter les mécanismes de protection de données sur le cloud AWS			**22% de l'évaluation globale de l'examen**	Examen en ligne avec une variété de questions (cf. détail plus haut) ** **Environ 38 minutes** (pour 10 à 12 questions évaluées) sont consacrées à cette compétence	Examen compensatoire, le taux de bonnes réponses doit être au **global** de **75% minimum**
	Concevoir et mettre en œuvre la gestion et l'utilisation des clés.	▸ Analyser un scénario donné pour déterminer une solution de gestion des clés appropriée. ▸ Compte tenu d'un ensemble d'exigences en matière de protection des données, évaluer l'utilisation des clés et recommander les modifications requises. ▸ Déterminer et contrôlez le rayon d'explosion d'un événement de compromis clé et concevoir une solution pour le contenir. ▸ Appliquer les différents types de cryptage des données « au repos » (du côté du client et du serveur par AWS) et en transit. ▸ Utiliser AWS Key Management Service (AWS KMS) pour créer et contrôler des clés de cryptage avec un service majoritairement géré par AWS. ▸ Utiliser AWS CloudHSM pour générer, stocker, importer, exporter et gérer des clés de cryptage (symétriques et asymétriques).			

	Résoudre les problèmes de gestion des clés.	▸ Gérer et modifier les politiques d'accès des clés en fonction des besoins et des problèmes affairant aux clés. ▸ Déterminer quand et comment révoquer les autorisations d'un utilisateur ou d'un service en cas de compromis. ▸ Supprimer une clé client / « customer key » en cas d'intégrité menacée.			
	Concevoir et mettre en œuvre une solution de cryptage des données pour les données au repos et les données en transit.	▸ Compte tenu d'un ensemble d'exigences en matière de protection des données, évaluer la sécurité des données au repos dans une charge de travail et recommander les modifications requises. ▸ Vérifier la stratégie d'une clé de manière à ce qu'elle ne puisse être utilisée que par des services AWS spécifiques. ▸ Appliquer les différents types de cryptage des données « au repos » (du côté du client et du serveur par AWS) et en transit. ▸ Utiliser IPsec avec une connectivité VPN pour faciliter le cryptage des données en transit. ▸ Utiliser AWS pour générer, déployer et gérer des certificats publics et prives utilises pour le cryptage TLS des charges de travail sur le net. ▸ Renforcer les contrôles de conformité avec des politiques « verrouillage de coffres »/« vault lock » pour les données stockées dans Amazon S3 Glacier. ▸ Utiliser Amazon Macie pour automatiquement découvrir, classifier et protéger les informations sensibles stockées sur AWS grâce au machine learning.			