Guide de l'examen AWS Certified Security - Specialty (SCS-C02)

Introduction

L'examen AWS Certified Security - Specialty (SCS-C02) est destiné aux personnes qui occupent un rôle en lien avec la sécurité. Cet examen valide la capacité du candidat à démontrer efficacement les connaissances qu'il a acquises en matière de sécurisation des produits et services AWS.

L'examen permet également de vérifier si un candidat possède les compétences suivantes :

- Compréhension des classifications des données spécialisées et des mécanismes de protection des données AWS
- Compréhension des méthodes de chiffrement des données et des mécanismes AWS permettant de les implémenter
- Compréhension des protocoles Internet sécurisés et des mécanismes AWS permettant de les implémenter
- Connaissance pratique des services de sécurité AWS et des fonctions des services pour fournir un environnement de production sécurisé
- Compétences justifiées par au moins deux ans d'expérience de déploiement en production avec les services et fonctions de sécurité AWS
- Capacité à trouver des compromis concernant les coûts, la sécurité et la complexité du déploiement afin de respecter les exigences d'une application
- Compréhension des opérations de sécurité et des risques

Description du candidat cible

Le candidat cible doit avoir l'équivalent de 3 à 5 ans d'expérience en sécurité informatique dans la conception et la mise en œuvre de solutions de sécurité. En outre, le candidat cible doit avoir au moins deux ans d'expérience pratique dans la sécurisation des charges de travail AWS.

Connaissances AWS recommandées

Le candidat cible doit maîtriser les sujets suivants :

- Modèle de responsabilité partagée AWS et application de ce modèle

- Connaissance générale des services AWS et du déploiement de solutions cloud
- Contrôles de sécurité pour les environnements et charges de travail AWS
- Stratégies de journalisation et de surveillance
- Gestion des vulnérabilités et automatisation de la sécurité
- Méthodes d'intégration des services de sécurité AWS avec des outils tiers
- Contrôles de reprise après sinistre, notamment les stratégies de sauvegarde
- Chiffrement et gestion des clés
- Gestion des identités et des accès
- Conservation des données et gestion du cycle de vie
- Procédures de résolution des problèmes de sécurité
- Gouvernance multicompte et conformité organisationnelle
- Stratégies de détection des menaces et de réponse aux incidents

Tâches extérieures au cadre des exigences pour le candidat cible

La liste suivante contient les tâches que le candidat cible n'est pas censé être en mesure d'effectuer. Cette liste n'est pas exhaustive. Ces tâches sortent du champ de l'examen :

- Développer des logiciels dans un langage spécifique (par exemple, Python, Java).
- Confirmer la conformité réglementaire.
- Gérer les cycles de vie du développement logiciel.
- Concevoir des topologies de réseau.
- Concevoir l'architecture de déploiements cloud globaux.
- Configurer des services de stockage en fonction des exigences de résidence des données (par exemple, le Règlement général sur la protection des données, ou RGPD).

Vous trouverez en annexe une liste de technologies et de concepts susceptibles de figurer dans l'examen, une liste des services et fonctions AWS inclus dans le champ de l'examen et une liste des services et fonctions AWS exclus du champ de l'examen.

Contenu de l'examen

Types de réponses

L'examen comporte deux types de questions :

- **Choix multiple :** une réponse correcte et trois réponses incorrectes (réponses piège)
- **Réponse multiple :** plusieurs réponses correctes sur cinq options de réponse ou plus

Sélectionnez une ou plusieurs réponses qui complètent l'affirmation ou répondent à la question. Les réponses piège, ou réponses incorrectes, sont des options qu'un candidat ayant des connaissances ou compétences incomplètes est susceptible de choisir. Les réponses piège sont généralement des réponses plausibles qui correspondent au contenu.

Les questions sans réponse sont notées comme incorrectes ; aucune pénalité n'est appliquée lorsque le candidat devine une réponse. L'examen comporte 50 questions qui ont une incidence sur votre score.

Contenu non noté

L'examen comporte 15 questions non notées qui n'ont pas d'incidence sur votre score. AWS recueille des informations sur les performances dans le cadre de ces questions non notées. L'objectif est d'évaluer ces questions en vue d'une utilisation ultérieure en tant que questions notées. Ces questions non notées ne sont pas identifiées comme telles dans l'examen.

Résultats de l'examen

L'examen AWS Certified Security - Specialty (SCS-C02) est sanctionné par une réussite ou un échec. L'examen est évalué selon une norme minimale établie par les professionnels d'AWS. Ceux-ci observent les bonnes pratiques et directives en matière de certification.

Vos résultats à l'examen sont présentés sous la forme d'un score gradué de 100 à 1 000. Le score minimal pour réussir est de 750. Votre score indique vos performances lors de l'examen dans son ensemble et si vous avez réussi l'examen. Les modèles de

score gradué permettent de mettre en correspondance des scores de différents formulaires d'examen qui peuvent présenter des niveaux de difficulté légèrement différents.

Votre compte-rendu de score peut contenir un tableau des classifications de vos performances au niveau de chaque section. L'examen utilise un modèle de notation compensatoire, ce qui signifie que vous n'avez pas besoin d'obtenir une note minimale dans chaque section. Vous devez seulement réussir l'examen dans son ensemble.

Chaque section de l'examen présente une pondération spécifique. Certaines sections comportent donc plus de questions que d'autres. Le tableau des classifications contient des informations générales qui mettent en évidence vos points forts et vos points faibles. Les commentaires au niveau des sections doivent être interprétés avec précaution.

Aperçu du contenu

Ce guide de l'examen inclut les pondérations, les domaines du contenu, ainsi que les énoncés de tâche de l'examen. Ce guide ne fournit pas une liste exhaustive du contenu de l'examen. Cependant, chaque énoncé de tâche est accompagné d'un contexte supplémentaire pour vous aider à vous préparer à l'examen.

L'examen comporte les domaines de contenu et les pondérations suivants :

- Domaine 1 : Détection des menaces et réponse aux incidents (14 % du contenu noté)
- Domaine 2 : Journalisation et surveillance de la sécurité (18 % du contenu noté)
- Domaine 3 : Sécurité de l'infrastructure (20 % du contenu noté)
- Domaine 4 : Gestion des identités et des accès (16 % du contenu noté)
- Domaine 5 : Protection des données (18 % du contenu noté)
- Domaine 6 : Gouvernance de la gestion et de la sécurité (14 % du contenu noté)

Domaine 1 : Détection des menaces et réponse aux incidents

Énoncé de la tâche 1.1 : Concevoir et mettre en œuvre un plan de réponse aux incidents.

Connaissance des éléments suivants :

- Bonnes pratiques d'AWS pour la réponse aux incidents
- Incidents liés au cloud
- Rôles et responsabilités dans le plan de réponse aux incidents
- Format de recherche de sécurité AWS (ASFF)

Compétences dans les domaines suivants :

- Mise en œuvre de stratégies d'invalidation et de rotation des justificatifs en réponse aux compromissions (par exemple, en utilisant AWS Identity and Access Management [IAM] et AWS Secrets Manager)
- Isolation des ressources AWS
- Conception et mise en œuvre de playbooks et de runbooks pour les réponses aux incidents de sécurité
- Déploiement de services de sécurité (par exemple, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- Configuration des intégrations avec les services AWS natifs et les services tiers (par exemple, en utilisant Amazon EventBridge et l'ASFF)

Énoncé de la tâche 1.2 : Détecter les menaces et les anomalies de sécurité en utilisant les services AWS.

Connaissance des éléments suivants :

- Services de sécurité gérés par AWS qui détectent les menaces
- Techniques relatives aux anomalie et à la corrélation pour relier les données entre les services
- Visualisations pour identifier les anomalies
- Stratégies de centralisation des résultats de sécurité

Compétences dans les domaines suivants :

- Évaluation des résultats des services de sécurité (par exemple, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)

- Recherche et corrélation des menaces de sécurité dans les services AWS (par exemple, à l'aide de Detective)
- Exécution de requêtes pour valider les événements de sécurité (par exemple, en utilisant Amazon Athena)
- Création de filtres de métriques et de tableaux de bord pour détecter les activités anormales (par exemple, en utilisant Amazon CloudWatch)

Énoncé de la tâche 1.3 : Réagir à la compromission des ressources et des charges de travail.

Connaissance des éléments suivants :

- Guide de réaction aux incidents de sécurité AWS
- Mécanismes d'isolation des ressources
- Techniques d'analyse des causes profondes
- Mécanismes de saisie de données
- Analyse des journaux pour la validation des événements

Compétences dans les domaines suivants :

- Automatisation de la remédiation à l'aide des services AWS (par exemple, AWS Lambda, AWS Step Functions, EventBridge, les runbooks AWS Systems Manager, Security Hub, AWS Config)
- Réponse à la compromission de ressources (par exemple, en isolant les instances Amazon EC2)
- Enquête et analyse pour effectuer une analyse des causes profondes (par exemple, en utilisant Detective)
- Capture de données d'analyse scientifique pertinentes à partir d'une ressource compromise (par exemple, instantanés de volumes Amazon Elastic Block Store [Amazon EBS], vidage de la mémoire)
- Interrogation des journaux dans Amazon S3 pour obtenir des informations contextuelles liées aux événements de sécurité (par exemple, en utilisant Athena)
- Protection et conservation des artefacts d'analyse scientifique (par exemple, en utilisant le verrouillage d'objets S3, les comptes d'analyse scientifique isolés, le cycle de vie S3 et la réplication S3)
- Préparation des services aux incidents et récupération des services après les incidents

Domaine 2 : Journalisation et surveillance de la sécurité

Énoncé de la tâche 2.1 : Concevoir et mettre en œuvre la surveillance et la génération d'alertes pour traiter les événements de sécurité.

Connaissance des éléments suivants :

- Services AWS qui surveillent les événements et fournissent des alarmes (par exemple, CloudWatch, EventBridge)
- Services AWS qui automatisent les alertes (par exemple, Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub)
- Outils qui surveillent les métriques et les bases de référence (par exemple, GuardDuty, Systems Manager)

Compétences dans les domaines suivants :

- Analyse des architectures pour identifier les exigences de surveillance et les sources de données pour la surveillance de la sécurité
- Analyse des environnements et des charges de travail afin de déterminer les besoins de surveillance
- Conception de la surveillance de l'environnement et de la charge de travail en fonction des exigences de l'entreprise et de la sécurité
- Mise en place d'outils et de scripts automatisés pour effectuer des audits réguliers (par exemple, en créant des insights personnalisés dans Security Hub)
- Définition des métriques et des seuils qui génèrent des alertes

Énoncé de la tâche 2.2 : Résoudre les problèmes liés aux alertes et à la surveillance de la sécurité.

Connaissance des éléments suivants :

- Configuration des services de surveillance (par exemple, Security Hub)
- Données pertinentes qui indiquent des événements de sécurité

Compétences dans les domaines suivants :

- Analyse de la fonctionnalité des services, des autorisations et de la configuration des ressources après un événement qui n'a pas fourni de visibilité ou d'alerte
- Analyse et correction de la configuration d'une application personnalisée qui ne génère pas de rapport de ses statistiques

- Évaluation des services de journalisation et de surveillance à aligner sur les exigences de sécurité

Énoncé de la tâche 2.3 : Concevoir et implémenter une solution de journalisation.

Connaissance des éléments suivants :

- Services et fonctionnalités AWS offrant des fonctions de journalisation (par exemple, journaux de flux VPC, journaux DNS, AWS CloudTrail, Amazon CloudWatch Logs)
- Attributs des capacités de journalisation (par exemple, niveaux de journalisation, type, verbosité)
- Destinations des journaux et gestion du cycle de vie (par exemple, période de conservation)

Compétences dans les domaines suivants :

- Configuration de la journalisation pour les services et les applications
- Identification des besoins en matière de journalisation et des sources d'ingestion des journaux
- Mise en œuvre du stockage des journaux et de la gestion du cycle de vie conformément aux bonnes pratiques d'AWS et aux exigences de l'organisation

Énoncé de la tâche 2.4 : Résoudre les problèmes liés aux solutions de journalisation.

Connaissance des éléments suivants :

- Capacités et cas d'utilisation des services AWS qui fournissent des sources de données (par exemple, le niveau, le type, la verbosité, le rythme, la régularité et l'immuabilité des journaux)
- Services et fonctionnalités AWS offrant des fonctions de journalisation (par exemple, journaux des flux VPC, journaux DNS, CloudTrail, CloudWatch Logs)
- Autorisations d'accès nécessaires à la journalisation

Compétences dans les domaines suivants :

- Identification d'une mauvaise configuration et détermination des étapes de remédiation pour les autorisations d'accès manquantes qui sont nécessaires pour la journalisation (par exemple, en gérant les autorisations de

lecture/écriture, les autorisations de compartiment S3, l'accès public et l'intégrité)
- Détermination de la cause des journaux manquants et exécution des étapes de remédiation

Énoncé de la tâche 2.5 : Concevoir une solution d'analyse des journaux.

Connaissance des éléments suivants :
- Services et outils permettant d'analyser les journaux capturés (par exemple, Athena, filtre CloudWatch Logs)
- Fonctions d'analyse des journaux des services AWS (par exemple, CloudWatch Logs Insights, CloudTrail Insights, Security Hub insights)
- Format et composants des journaux (par exemple, les journaux CloudTrail)

Compétences dans les domaines suivants :
- Identification de schémas dans les journaux pour indiquer des anomalies et des menaces connues
- Normalisation, analyse et mise en corrélation des journaux

Domaine 3 : Sécurité de l'infrastructure

Énoncé de la tâche 3.1 : Concevoir et mettre en œuvre des contrôles de sécurité pour les services périphériques.

Connaissance des éléments suivants :
- Fonctions de sécurité sur les services périphériques (par exemple, AWS WAF, équilibreurs de charge, Amazon Route 53, Amazon CloudFront, AWS Shield)
- Attaques, menaces et failles courantes (par exemple, Top 10 de l'Open Web Application Security Project [OWASP], attaque par déni de service (DDoS))
- Architecture d'application web en couches

Compétences dans les domaines suivants :
- Définition de stratégies de sécurité périphérique pour les cas d'utilisation courants (par exemple, site web public, application serverless, backend d'application mobile)
- Sélection de services périphériques appropriés en fonction des menaces et des attaques prévues (par exemple, Top 10 OWASP, attaque par déni de service (DDoS))

- Sélection de protections appropriées en fonction des vulnérabilités et des risques anticipés (par exemple, logiciels, applications et bibliothèques vulnérables)
- Définition de couches de défense en combinant des services de sécurité périphérique (par exemple, CloudFront avec AWS WAF et des équilibreurs de charge)
- Application de restrictions à la périphérie en fonction de divers critères (par exemple, la géographie, la géolocalisation, la limite de débit)
- Activation des journaux, des métriques et de la surveillance autour des services périphériques pour indiquer les attaques

Énoncé de la tâche 3.2 : Concevoir et mettre en œuvre des contrôles de sécurité réseau.

Connaissance des éléments suivants :

- Mécanismes de sécurité VPC (par exemple, groupes de sécurité, ACL réseau, AWS Network Firewall)
- Connectivité inter-VPC (par exemple, AWS Transit Gateway, points de terminaison VPC)
- Sources de télémétrie de sécurité (par exemple, mise en miroir du trafic, journaux de flux VPC)
- Technologie, terminologie et utilisation des VPN
- Options de connectivité sur site (par exemple, AWS VPN, AWS Direct Connect)

Compétences dans les domaines suivants :

- Mise en œuvre de la segmentation du réseau en fonction des exigences de sécurité (par exemple, sous-réseaux publics, sous-réseaux privés, VPC sensibles, connectivité sur site)
- Conception de contrôles de réseau pour autoriser ou bloquer le trafic réseau selon les besoins (par exemple, en utilisant des groupes de sécurité, des ACL réseau et Network Firewall)
- Conception de flux de réseau pour maintenir les données hors de l'Internet public (par exemple, en utilisant Transit Gateway, les points de terminaison VPC et Lambda dans les VPC)

- Détermination des sources de télémétrie à surveiller en fonction de la conception du réseau, des menaces et des attaques (par exemple, journaux des équilibreurs de charge, journaux de flux VPC, mise en miroir du trafic)
- Détermination des exigences en matière de redondance et de charge de travail de sécurité pour la communication entre les environnements sur site et le cloud AWS (par exemple, en utilisant AWS VPN, AWS VPN via Direct Connect et MACsec)
- Identification et suppression des accès réseau inutiles
- Gestion des configurations réseau face à l'évolution des exigences (par exemple, à l'aide d'AWS Firewall Manager)

Énoncé de la tâche 3.3 : Concevoir et mettre en œuvre des contrôles de sécurité pour les charges de travail de calcul.

Connaissance des éléments suivants :

- Mise en service et maintenance des instances EC2 (par exemple, correctifs, inspection, création d'instantanés et d'AMI, utilisation d'EC2 Image Builder)
- Rôles d'instance IAM et rôles de service IAM
- Services qui recherchent les vulnérabilités dans les charges de travail de calcul (par exemple, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR])
- Sécurité basée sur l'hôte (par exemple, pare-feu, renforcement)

Compétences dans les domaines suivants :

- Création d'AMI EC2 renforcées
- Application des rôles d'instance et des rôles de service nécessaires pour autoriser les charges de travail de calcul
- Analyse des instances EC2 et des images de conteneurs pour rechercher les vulnérabilités connues
- Application de correctifs sur une flotte d'instances EC2 ou d'images de conteneurs
- Activation des mécanismes de sécurité basés sur l'hôte (par exemple, les pare-feu basés sur l'hôte)
- Analyse des conclusions d'Amazon Inspector et détermination des techniques d'atténuation appropriées

- Transmission sécurisée de secrets et de justificatifs aux charges de travail de calcul

Énoncé de la tâche 3.4 : Résoudre les problèmes de sécurité du réseau.

Connaissance des éléments suivants :

- Analyse de l'accessibilité (par exemple, à l'aide de VPC Reachability Analyzer et d'Amazon Inspector)
- Concepts fondamentaux des réseaux TCP/IP (par exemple, UDP par rapport à TCP, ports, modèle d'interconnexion des systèmes ouverts [OSI], utilitaires de système d'exploitation de réseau)
- Lecture des sources de journaux pertinentes (par exemple, les journaux Route 53, les journaux AWS WAF, les journaux de flux VPC)

Compétences dans les domaines suivants :

- Identification, interprétation et hiérarchisation des problèmes de connectivité réseau (par exemple, en utilisant Amazon Inspector Network Reachability)
- Détermination des solutions pour obtenir le comportement souhaité du réseau
- Analyse des sources de journaux pour identifier les problèmes
- Capture d'échantillons de trafic pour l'analyse des problèmes (par exemple, en utilisant la mise en miroir du trafic)

Domaine 4 : Gestion des identités et des accès

Énoncé de la tâche 4.1 : Concevoir, mettre en œuvre et résoudre les problèmes d'authentification pour les ressources AWS.

Connaissance des éléments suivants :

- Méthodes et services de création et de gestion des identités (par exemple, fédération, fournisseurs d'identité, AWS IAM Identity Center [AWS Single Sign-On], Amazon Cognito)
- Mécanismes de délivrance de justificatifs à long terme et temporaires
- Résolution des problèmes d'authentification (par exemple, en utilisant CloudTrail, IAM Access Advisor et le simulateur de politique IAM)

Compétences dans les domaines suivants :

- Établissement de l'identité par le biais d'un système d'authentification, en fonction des exigences
- Configuration de l'authentification multifacteur (MFA)
- Détermination du moment opportun pour utiliser AWS Security Token Service (AWS STS) afin de délivrer des justificatifs temporaires

Énoncé de la tâche 4.2 : Concevoir, mettre en œuvre et résoudre les problèmes d'autorisation pour les ressources AWS.

Connaissance des éléments suivants :

- Différentes politiques IAM (par exemple, politiques gérées, politiques en ligne, politiques basées sur l'identité, politiques basées sur les ressources, politiques de contrôle des sessions)
- Composantes et impact d'une politique (par exemple, Principal, Action, Ressource, Condition)
- Résolution des problèmes d'autorisation (par exemple, en utilisant CloudTrail, IAM Access Advisor et le simulateur de politique IAM)

Compétences dans les domaines suivants :

- Élaboration de stratégies de contrôle d'accès basé sur les attributs (ABAC) et de contrôle d'accès basé sur les rôles (RBAC)
- Évaluation des types de politiques IAM en fonction des exigences et des charges de travail
- Interprétation de l'effet d'une politique IAM sur les environnements et les charges de travail
- Application du principe du moindre privilège dans un environnement
- Mise en œuvre d'une séparation adéquate des tâches
- Analyse des erreurs d'accès ou d'autorisation pour en déterminer la cause ou l'effet
- Enquête sur les permissions, autorisations ou privilèges non intentionnels accordés à une ressource, un service ou une entité

Domaine 5 : Protection des données

Énoncé de la tâche 5.1 : Concevoir et mettre en œuvre des contrôles qui assurent la confidentialité et l'intégrité des données en transit.

Connaissance des éléments suivants :

- Concepts TLS
- Concepts VPN (par exemple, IPsec)
- Méthodes d'accès à distance sécurisé (par exemple, SSH, RDP sur Systems Manager Session Manager)
- Concepts Systems Manager Session Manager
- Fonctionnement des certificats TLS avec les différents services et ressources du réseau (par exemple, CloudFront, équilibreurs de charge)

Compétences dans les domaines suivants :

- Conception d'une connectivité sécurisée entre AWS et les réseaux sur site (par exemple, à l'aide de Direct Connect et de passerelles VPN)
- Conception de mécanismes exigeant le chiffrement lors de la connexion aux ressources (par exemple, Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, équilibreurs de charge, Amazon Elastic File System [Amazon EFS], Amazon API Gateway)
- Exigence de TLS pour les appels d'API AWS (par exemple, avec Amazon S3)
- Conception de mécanismes permettant de transférer le trafic sur des connexions sécurisées (par exemple, en utilisant Systems Manager et EC2 Instance Connect)
- Conception de réseaux entre régions à l'aide de VIF privées et de VIF publiques

Énoncé de la tâche 5.2 : Concevoir et mettre en œuvre des contrôles qui assurent la confidentialité et l'intégrité des données au repos.

Connaissance des éléments suivants :

- Choix de la technique de chiffrement (par exemple, côté client, côté serveur, symétrique, asymétrique)
- Techniques de contrôle d'intégrité (par exemple, algorithmes de hachage, signatures numériques)

- Politiques de ressources (par exemple, pour DynamoDB, Amazon S3 et AWS Key Management Service [AWS KMS])
- Rôles et politiques IAM

Compétences dans les domaines suivants :

- Conception de politiques de ressources pour restreindre l'accès aux utilisateurs autorisés (par exemple, politiques de compartiment S3, politiques DynamoDB)
- Conception de mécanismes pour empêcher l'accès public non autorisé (par exemple, S3 Block Public Access, prévention des instantanés publics et des AMI publiques)
- Configuration de services pour activer le chiffrement des données au repos (par exemple, Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS)
- Conception de mécanismes visant à protéger l'intégrité des données en empêchant les modifications (par exemple, en utilisant le verrouillage des objets S3, les politiques relatives aux clés KMS, le verrouillage de coffre S3 Glacier et le verrouillage de coffre AWS Backup)
- Conception du chiffrement au repos en utilisant AWS CloudHSM pour les bases de données relationnelles (par exemple, Amazon RDS, RDS Custom, bases de données sur des instances EC2)
- Choix des techniques de chiffrement en fonction des exigences de l'entreprise

Énoncé de la tâche 5.3 : Concevoir et mettre en œuvre des contrôles pour gérer le cycle de vie des données au repos.

Connaissance des éléments suivants :

- Stratégies de cycle de vie
- Normes de conservation des données

Compétences dans les domaines suivants :

- Conception de mécanismes de cycle de vie S3 pour conserver les données pendant les périodes de conservation requises (par exemple, verrouillage des objets S3, verrouillage de coffre S3 Glacier, politique de cycle de vie S3)
- Conception de la gestion automatique du cycle de vie des services et ressources AWS (par exemple, Amazon S3, instantanés de volume EBS,

instantanés de volume RDS, AMI, images de conteneur, groupes de journaux CloudWatch, Amazon Data Lifecycle Manager)
- Établissement de calendriers et de la conservation pour AWS Backup dans les services AWS

Énoncé de la tâche 5.4 : Concevoir et mettre en œuvre des contrôles pour protéger les justificatifs, les secrets et les clés de chiffrement.

Connaissance des éléments suivants :
- Secrets Manager
- Systems Manager Parameter Store
- Utilisation et gestion de clés symétriques et asymétriques (par exemple, AWS KMS)

Compétences dans les domaines suivants :
- Conception de la gestion et de la rotation des secrets pour les charges de travail (par exemple, les justificatifs d'accès aux bases de données, les clés API, les clés d'accès IAM, les clés gérées par le client AWS KMS)
- Conception de politiques de clés KMS pour limiter l'utilisation des clés aux utilisateurs autorisés
- Mise en place de mécanismes permettant d'importer et de supprimer un élément de clé fourni par le client

Domaine 6 : Gouvernance de la gestion et de la sécurité

Énoncé de la tâche 6.1 : Élaborer une stratégie pour déployer et gérer de manière centralisée les comptes AWS.

Connaissance des éléments suivants :
- Stratégies multicomptes
- Services gérés qui permettent une administration déléguée
- Garde-fous définis par une politique
- Bonnes pratiques relatives au compte racine
- Rôles devant être partagés entre les comptes

Compétences dans les domaines suivants :

- Déploiement et configuration d'AWS Organizations
- Détermination du moment et de la manière de déployer AWS Control Tower (par exemple, quels services doivent être désactivés pour un déploiement réussi)
- Mise en œuvre des SCP comme solution technique pour appliquer une politique (par exemple, limitations de l'utilisation d'un compte racine, mise en place de contrôles dans AWS Control Tower)
- Gestion centralisée des services de sécurité et agrégation des résultats (par exemple, en utilisant l'administration déléguée et les agrégateurs AWS Config)
- Sécurisation des justificatifs de l'utilisateur racine/administrateur du compte AWS

Énoncé de la tâche 6.2 : Mettre en œuvre une stratégie de déploiement sécurisée et cohérente pour les ressources cloud.

Connaissance des éléments suivants :

- Bonnes pratiques de déploiement avec Infrastructure as code (IaC) (par exemple, renforcement des modèles AWS CloudFormation et détection des écarts)
- Bonnes pratiques en matière de balisage
- Gestion, déploiement et gestion des versions centralisés des services AWS
- Visibilité et contrôle de l'infrastructure AWS

Compétences dans les domaines suivants :

- Utilisation de CloudFormation pour déployer des ressources de cloud de manière cohérente et sécurisée
- Mise en œuvre et application de stratégies de balisage multi-comptes
- Configuration et déploiement de portefeuilles de services AWS approuvés (par exemple, à l'aide d'AWS Service Catalog)
- Organisation des ressources AWS en différents groupes pour la gestion
- Déploiement de Firewall Manager pour appliquer les politiques
- Partage sécurisé des ressources entre les comptes AWS (par exemple, à l'aide d'AWS Resource Access Manager [AWS RAM])

Énoncé de la tâche 6.3 : Évaluer la conformité des ressources AWS.

Connaissance des éléments suivants :

- Classification des données à l'aide des services AWS
- Évaluation, audit, et analyse des configurations des ressources AWS (par exemple, en utilisant AWS Config)

Compétences dans les domaines suivants :

- Identification des données sensibles à l'aide de Macie
- Création de règles AWS Config pour la détection des ressources AWS non conformes
- Collecte et organisation des preuves à l'aide de Security Hub et d'AWS Audit Manager

Énoncé de la tâche 6.4 : Identifier les lacunes en matière de sécurité par des examens de l'architecture et une analyse des coûts.

Connaissance des éléments suivants :

- Coût et utilisation d'AWS pour l'identification des anomalies
- Stratégies pour réduire les surfaces d'attaque
- AWS Well-Architected Framework

Compétences dans les domaines suivants :

- Identification des anomalies sur la base de l'utilisation des ressources et des tendances
- Identification des ressources inutilisées à l'aide des services et outils AWS (par exemple, AWS Trusted Advisor, AWS Cost Explorer)
- Utilisation de l'outil AWS Well-Architected Tool pour identifier les failles de sécurité

Annexe

Technologies et concepts susceptibles de figurer dans l'examen

La liste suivante contient les technologies et les concepts susceptibles de figurer dans l'examen. Cette liste n'est pas exhaustive et peut faire l'objet de modifications. L'ordre et l'emplacement des éléments de cette liste ne constituent pas une indication de leur poids relatif ou de leur importance relative dans le cadre de l'examen :

- Interface AWS CLI
- Kits AWS SDK
- Console de gestion AWS
- Accès à distance sécurisé
- Gestion des certificats
- Infrastructure as code (IaC)

Services et fonctions AWS concernés

Remarque : La sécurité a un impact sur tous les services AWS. De nombreux services ne figurent pas dans cette liste car le service global sort du champ de l'examen, mais les aspects du service liés à la sécurité sont concernés. Par exemple, les candidats à cet examen ne seront pas interrogés sur les étapes à suivre pour configurer la réplication pour un compartiment S3. Toutefois, les candidats peuvent être interrogés sur la configuration d'une politique de compartiment S3.

La liste suivante contient les services et fonctions AWS qui font partie du champ de l'examen. Cette liste n'est pas exhaustive et peut faire l'objet de modifications. Les offres AWS apparaissent dans des catégories correspondant à leurs fonctions principales :

Gestion et gouvernance :

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Organizations
- AWS Systems Manager
- AWS Trusted Advisor

Réseaux et diffusion de contenu :

- Amazon VPC
  - Analyseur d'accès réseau
  - Listes ACL réseau
  - Groupes de sécurité
  - Points de terminaison d'un VPC

Sécurité, identité et conformité :

- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS IAM Identity Center (AWS Single Sign-On)
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- AWS WAF

Services et fonctions AWS hors du champ de l'examen

La liste suivante contient les services et fonctions AWS qui sont hors du champ de l'examen. Cette liste n'est pas exhaustive et peut faire l'objet de modifications. Les offres AWS qui ne sont aucunement liées aux rôles cibles de l'examen sont exclues de cette liste :

Blockchain :

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database (Amazon QLDB)

Applications métier :

- Alexa for Business
- Amazon Chime
- Kit SDK Amazon Chime
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- Chaîne d'approvisionnement AWS
- AWS Wickr
- Amazon WorkDocs

Informatique pour l'utilisateur final :

- Amazon AppStream 2.0

Services multimédias :

- Amazon Elastic Transcoder
- AWS Elemental Appliances and Software
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Interactive Video Service (Amazon IVS)
- Amazon Kinesis Video Streams
- Amazon Nimble Studio

Migration et transfert :

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service (AWS DMS)
- Migration Evaluator
- AWS Migration Hub
- AWS Transfer Family

Technologies quantiques :

- Amazon Braket

Robotique :

- AWS RoboMaker

Satellite :

- AWS Ground Station

Enquête

Ce guide de l'examen vous a-t-il été utile ? Dites-nous ce que vous en pensez en répondant à notre enquête.