Guía de examen AWS Certified Security - Specialty (SCS-C02)

Introducción

El examen AWS Certified Security - Specialty (SCS-C02) está dirigido a personas que desempeñan un rol de seguridad. El examen valida la capacidad de un candidato para demostrar eficazmente sus conocimientos sobre seguridad en los productos y servicios de AWS.

El examen también valida si un candidato tiene lo siguiente:

- conocimiento de las clasificaciones de datos especializadas y los mecanismos de protección de datos de AWS
- conocimiento de los métodos de cifrado de datos y los mecanismos de AWS para implementarlos
- conocimiento de los protocolos seguros de Internet y los mecanismos de AWS para implementarlos
- conocimiento práctico de los servicios de seguridad de AWS y las funciones de los servicios para proporcionar un entorno de producción seguro
- competencia de 2 o más años de experiencia en implementación de producción en el uso de servicios de seguridad y funciones de AWS
- la capacidad de tomar decisiones compensatorias en relación con la complejidad, los costos, la seguridad y la implementación para cumplir un conjunto de requisitos de una aplicación
- comprensión de las operaciones de seguridad y los riesgos

Descripción del candidato objetivo

El candidato objetivo debe tener de 3a5 años de experiencia en el diseño e implementación de soluciones de seguridad. Además, el candidato objetivo debe tener un mínimo de 2 años de experiencia práctica en la protección de cargas de trabajo de AWS.

Conocimientos recomendados de AWS

El candidato objetivo debe tener los siguientes conocimientos:

- el modelo de responsabilidad compartida de AWS y su aplicación
- conocimientos generales sobre los servicios de AWS y la implementación de soluciones en la nube
- controles de seguridad para entornos y cargas de trabajo de AWS
- estrategias de registro y supervisión
- administración de vulnerabilidades y automatización de la seguridad
- formas de integrar los servicios de seguridad de AWS con herramientas de terceros
- controles de recuperación ante desastres, incluidas estrategias de respaldo
- criptografía y administración de claves
- administración de acceso a identidades
- retención de datos y administración del ciclo de vida
- cómo solucionar problemas de seguridad
- gobernanza de múltiples cuentas y conformidad de la organización
- estrategias de detección de amenazas y respuesta ante incidentes

Tareas de trabajo que están fuera del alcance del candidato

A continuación, se muestra una lista que contiene las tareas de trabajo que no se espera que el candidato pueda realizar. Esta lista no es exhaustiva. Estas tareas están fuera del alcance del examen:

- desarrollar software en un lenguaje específico (por ejemplo, Python, Java).
- confirmar la conformidad normativa.
- administrar los ciclos de vida del desarrollo de software.
- diseñar topologías de red.
- diseñar las implementaciones generales de la nube.
- configure los servicios de almacenamiento en función de los requisitos de residencia de los datos (por ejemplo, el Reglamento General de Protección de Datos [GDPR]).

Consulte el apéndice para obtener una lista de tecnologías y conceptos que pueden aparecer en el examen, una lista de los servicios y funciones de AWS dentro del alcance y una lista de los servicios y funciones de AWS fuera del alcance.

Contenido del examen

Tipos de respuesta

En el examen, hay dos tipos de preguntas:

- **Opciones múltiples:** hay una respuesta correcta y tres incorrectas (distractoras)
- **Respuesta múltiple:** hay dos o más respuestas correctas entre cinco o más opciones

Seleccione una o más respuestas que completen la afirmación o respondan a la pregunta de la mejor manera. Las distractoras, o respuestas incorrectas, son opciones que podría elegir un candidato que no tenga un buen nivel de conocimientos o habilidades. Por lo general, las distractoras son respuestas verosímiles que coinciden con el área de contenido.

Las preguntas sin respuesta se califican como incorrectas. No hay penalización por adivinar. El examen incluye 50 preguntas que afectarán la puntuación.

Contenido sin puntaje

El examen incluye 15 preguntas sin puntaje que no afectan la puntuación total. AWS recopila información sobre el desempeño en estas preguntas sin puntaje a fin de evaluarlas para su uso como preguntas con puntaje en el futuro. Estas preguntas sin puntaje no están identificadas en el examen.

Resultados del examen

El examen AWS Certified Security - Specialty (SCS-C02) es un examen que tiene una denominación de aprobado o reprobado. El puntaje se califica según un estándar mínimo que establecen los profesionales de AWS en función de las prácticas recomendadas y las pautas del sector de la certificación.

El informe de los resultados del examen es una puntuación en la escala del 100 al 1000. La puntuación mínima para aprobar es 750. La puntuación muestra cómo le fue en el examen en general y si lo aprobó o no. Los modelos de puntajes en escala ayudan a equiparar puntajes de varios formatos de examen que pueden tener niveles de dificultad un poco diferentes.

El informe del puntaje puede contener una tabla de clasificación de su desempeño en cada sección. En el examen, se usa un modelo de puntaje compensatorio, lo que significa que no es necesario aprobar cada sección. Solo necesita aprobar el examen general.

Cada sección del examen tiene una ponderación específica, por lo que algunas contienen más preguntas que otras. En la tabla de clasificaciones, se presenta información general que resalta sus fortalezas y debilidades. Interprete los comentarios de cada sección con prudencia.

Descripción del contenido

Esta guía de examen incluye ponderaciones, dominios de contenido y enunciados de tareas para el examen. Esta guía no proporciona una lista completa del contenido del examen. Sin embargo, hay un contexto adicional disponible de cada enunciado de tareas para ayudarlo a prepararse para el examen.

El examen tiene los siguientes dominios de contenido y ponderaciones:

- Dominio 1: Detección de amenazas y respuesta ante incidentes (14 % del contenido puntuado)
- Dominio 2: Registro y supervisión de seguridad (18 % del contenido puntuado)
- Dominio 3: Seguridad de infraestructura (20 % del contenido puntuado)
- Dominio 4: Identity and Access Management (16 % del contenido puntuado)
- Dominio 5: Protección de datos (18 % del contenido puntuado)
- Dominio 6: Administración y gobernanza de seguridad (14 % del contenido puntuado)

Dominio 1: Detección de amenazas y respuesta ante incidentes

Enunciado de la tarea 1.1: Diseñar e implementar un plan de respuesta ante incidentes.

Conocimientos de:

- prácticas recomendadas de AWS para la respuesta ante incidentes
- incidentes en la nube
- roles y responsabilidades en el plan de respuesta ante incidentes
- formato de búsqueda de seguridad de AWS (ASFF)

Habilidades para:

- implementar estrategias de invalidación y rotación de credenciales en respuesta a los compromisos (por ejemplo, mediante AWS Identity and Access Management [IAM] y AWS Secrets Manager)
- aislar los recursos de AWS
- diseñar e implementar manuales y manuales de procedimientos para respuestas a incidentes de seguridad
- implementar servicios de seguridad (por ejemplo, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- configurar integraciones con servicios nativos de AWS y servicios de terceros (por ejemplo, mediante Amazon EventBridge y ASFF)

Enunciado de la tarea 1.2: Detectar amenazas y anomalías de seguridad mediante los productos de AWS.

Conocimientos de:

- servicios de seguridad administrados de AWS que detectan amenazas
- técnicas de anomalías y correlación para unir datos entre servicios
- visualizaciones para identificar anomalías
- estrategias para centralizar los hallazgos de seguridad

Habilidades para:

- evaluar los hallazgos de los servicios de seguridad (por ejemplo, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)

- buscar y relacionar amenazas de seguridad en los servicios de AWS (por ejemplo, mediante Detective)
- realizar consultas para validar eventos de seguridad (por ejemplo, mediante Amazon Athena)
- crear filtros de métricas y paneles para detectar actividades anómalas (por ejemplo, mediante Amazon CloudWatch)

Enunciado de la tarea 1.3: Responder a los recursos y cargas de trabajo comprometidos.

Conocimientos de:

- guía de respuesta ante incidentes de seguridad en AWS
- mecanismos de aislamiento de recursos
- técnicas para el análisis de la causa raíz
- mecanismos de captura de datos
- análisis de registros para la validación de eventos

Habilidades para:

- automatizar la corrección mediante el uso de los servicios de AWS (por ejemplo, AWS Lambda, AWS Step Functions, EventBridge, los manuales de procedimientos de AWS Systems Manager, Security Hub, AWS Config)
- responder a los recursos comprometidos (por ejemplo, aislando las instancias de Amazon EC2)
- investigar y examinar para analizar la causa raíz (por ejemplo, mediante Detective)
- capturar datos forenses relevantes de un recurso comprometido (por ejemplo, instantáneas de volumen de Amazon Elastic Block Store [Amazon EBS], volcado de memoria)
- consultar los registros de Amazon S3 para obtener información contextual relacionada con los eventos de seguridad (por ejemplo, mediante Athena)
- proteger y preservar los artefactos forenses (por ejemplo, mediante bloqueo de objetos de S3, las cuentas forenses aisladas, S3 Lifecycle y la replicación de S3)
- preparar los servicios para los incidentes y recuperar los servicios después de los incidentes

Dominio 2: Registro y supervisión de seguridad

Enunciado de la tarea 2.1: Diseñar e implementar la supervisión y las alertas para abordar los eventos de seguridad.

Conocimientos de:

- servicios de AWS que supervisan los eventos y proporcionan alarmas (por ejemplo, CloudWatch, EventBridge)
- servicios de AWS que automatizan las alertas (por ejemplo, Lambda, Amazon Simple Notification Service [Amazon SNS] o Security Hub)
- herramientas que supervisan las métricas y las bases de referencia (por ejemplo, GuardDuty, Systems Manager)

Habilidades para:

- analizar las arquitecturas para identificar los requisitos de supervisión y las fuentes de datos para la supervisión de la seguridad
- analizar los entornos y las cargas de trabajo para determinar los requisitos de supervisión
- diseñar la supervisión del entorno y de la carga de trabajo en función de los requisitos empresariales y de seguridad
- configurar las herramientas y scripts automatizados para realizar auditorías periódicas (por ejemplo, mediante la creación de información personalizada en Security Hub)
- definir las métricas y los umbrales que generan alertas

Enunciado de la tarea 2.2: Solucionar problemas de monitoreo y alertas de seguridad.

Conocimientos de:

- configuración de los servicios de supervisión (por ejemplo, Security Hub)
- datos relevantes que indican eventos de seguridad

Habilidades para:

- analizar la funcionalidad del servicio, los permisos y la configuración de los recursos después de un evento que no proporcionó visibilidad ni alertas
- analizar y corregir la configuración de una aplicación personalizada que no presenta sus estadísticas
- evaluar los servicios de registro y supervisión para alinearlos con los requisitos de seguridad

Enunciado de la tarea 2.3: Diseñar e implementar una solución de registro.

Conocimientos de:

- servicios y funciones de AWS que proporcionan capacidades de registro (por ejemplo, registros de flujo de VPC, registros de DNS, AWS CloudTrail, Amazon CloudWatch Logs)
- atributos de las capacidades de registro (por ejemplo, niveles de registro, tipo, nivel de detalle)
- administración de los destinos y del ciclo de vida de los registros (por ejemplo, el periodo de retención)

Habilidades para:

- configurar el registro para servicios y aplicaciones
- identificar los requisitos de registro y las fuentes para la ingesta de registros
- implementar el almacenamiento de registros y la administración del ciclo de vida de acuerdo con las prácticas recomendadas de AWS y los requisitos de la organización

Enunciado de la tarea 2.4: Solucionar problemas de soluciones de registro.

Conocimientos de:

- capacidades y casos prácticos de los servicios de AWS que proporcionan orígenes de datos (por ejemplo, nivel de registro, tipo, nivel de detalle, cadencia, puntualidad, inmutabilidad)
- servicios y funciones de AWS que proporcionan capacidades de registro (por ejemplo, registros de flujo de VPC, registros de DNS, CloudTrail, CloudWatch Logs)
- permisos de acceso necesarios para el registro

Habilidades para:

- identificar los errores de configuración y determinar los pasos para corregir los permisos de acceso ausentes que son necesarios para el registro (por ejemplo, mediante la administración de los permisos de lectura/escritura, los permisos de *bucket* de S3, el acceso público y la integridad)
- determinar la causa de la falta de registros y realizar los pasos de corrección

Enunciado de la tarea 2.5: Diseñar una solución de análisis de registros.

Conocimientos de:

- servicios y herramientas para analizar los registros capturados (por ejemplo, Athena, el filtro de CloudWatch Logs)
- funciones de análisis de registros de los servicios de AWS (por ejemplo, información de registros, información de Cloudtrail, información de Security Hub)
- formato y componentes de registro (por ejemplo, registros de CloudTrail)

Habilidades para:

- identificar patrones en los registros para indicar anomalías y amenazas conocidas
- normalizar, analizar y correlacionar registros

Dominio 3: Seguridad de la infraestructura

Enunciado de la tarea 3.1: Diseñar e implementar controles de seguridad para los servicios perimetrales.

Conocimientos de:

- funciones de seguridad en los servicios perimetrales (por ejemplo, AWS WAF, equilibradores de carga, Amazon Route 53, Amazon CloudFront, AWS Shield)
- ataques, amenazas y vulnerabilidades comunes (por ejemplo, los 10 mejores del Proyecto abierto de seguridad de aplicaciones web [OWASP, Open Web Application Security Project], DDoS)
- arquitectura de aplicaciones web en capas

Habilidades para:

- definir estrategias de seguridad perimetral para casos prácticos comunes (por ejemplo, sitios web públicos, aplicaciones sin servidor, *backend* de aplicaciones móviles)
- seleccionar los servicios perimetrales adecuados en función de las amenazas y los ataques anticipados (por ejemplo, los 10 principales de OWASP, DDoS)
- seleccionar las protecciones adecuadas en función de las vulnerabilidades y los riesgos previstos (por ejemplo, software, aplicaciones o bibliotecas vulnerables)

- definir capas de defensa mediante la combinación de servicios de seguridad perimetrales (por ejemplo, CloudFront con AWS WAF y equilibradores de carga)
- aplicar restricciones en el perímetro en función de varios criterios (por ejemplo, la geografía, la geolocalización, el límite de tarifas)
- activar los registros, las métricas y la supervisión de los servicios perimetrales para indicar los ataques

Enunciado de la tarea 3.2: Diseñar e implementar controles de seguridad de red.

Conocimientos de:

- mecanismos de seguridad de VPC (por ejemplo, grupos de seguridad, ACL de red, AWS Network Firewall)
- conectividad entre VPC (por ejemplo, AWS Transit Gateway, puntos de enlace de VPC)
- fuentes de telemetría de seguridad (por ejemplo, Traffic Mirroring o registros de flujo de VPC)
- tecnología, terminología y uso de VPN
- opciones de conectividad en las instalaciones (por ejemplo, AWS VPN, AWS Direct Connect)

Habilidades para:

- implementar la segmentación de la red en función de los requisitos de seguridad (por ejemplo, subredes públicas, subredes privadas, VPC confidenciales, conectividad en las instalaciones)
- diseñar controles de red para permitir o impedir el tráfico de red según sea necesario (por ejemplo, mediante grupos de seguridad, ACL de red y Network Firewall)
- diseñar flujos de red para mantener los datos fuera de la internet pública (por ejemplo, mediante el uso de Transit Gateway, los puntos de enlace de VPC y Lambda en las VPC)
- determinar qué fuentes de telemetría se deben supervisar en función del diseño de la red, las amenazas y los ataques (por ejemplo, los registros del equilibrador de carga, los registros de flujo de VPC, Traffic Mirroring)
- determinar los requisitos de redundancia y carga de trabajo de seguridad para la comunicación entre los entornos en las instalaciones y la nube de

AWS (por ejemplo, mediante AWS VPN, AWS VPN a través de Direct Connect y MACSec)
- identificar y eliminar el acceso innecesario a la red
- administrar las configuraciones de red a medida que cambian los requisitos (por ejemplo, mediante AWS Firewall Manager)

Enunciado de la tarea 3.3: Diseñar e implementar controles de seguridad para las cargas de trabajo de cómputo.

Conocimientos de:
- aprovisionamiento y mantenimiento de instancias de EC2 (por ejemplo, aplicación de parches, inspección, creación de instantáneas y AMI, uso de EC2 Image Builder)
- roles de instancia de IAM y funciones del servicio de IAM
- servicios que buscan vulnerabilidades en las cargas de trabajo de cómputo (por ejemplo, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR])
- seguridad basada en host (por ejemplo, firewalls, refuerzo)

Habilidades para:
- crear AMI de EC2 reforzadas
- aplicar los roles de instancia y las funciones del servicio según corresponda para autorizar las cargas de trabajo de cómputo
- analizar instancias de EC2 e imágenes de contenedores para detectar vulnerabilidades conocidas
- aplicar parches en una flota de instancias de EC2 o imágenes de contenedores
- activar los mecanismos de seguridad basados en el host (por ejemplo, los firewalls basados en el host)
- analizar los hallazgos de Amazon Inspector y determinar las técnicas de mitigación adecuadas
- transmitir secretos y credenciales de forma segura a las cargas de trabajo de cómputo

Enunciado de la tarea 3.4: Solucionar problemas de seguridad de la red.

Conocimientos de:

- cómo analizar la conectividad (por ejemplo, mediante VPC Reachability Analyzer y Amazon Inspector)
- conceptos fundamentales de redes TCP/IP (por ejemplo, UDP en comparación con TCP, puertos, modelo de interconexión de sistemas abiertos [OSI], utilidades del sistema operativo de red)
- cómo leer las fuentes de registro relevantes (por ejemplo, los registros de Route 53, los registros de AWS WAF y los registros de flujo de VPC)

Habilidades para:

- identificar, interpretar y priorizar los problemas de conectividad de red (por ejemplo, mediante conexiones de red de Amazon Inspector)
- determinar soluciones para producir el comportamiento de red deseado
- analizar las fuentes de registro para identificar problemas
- capturar muestras de tráfico para analizar problemas (por ejemplo, mediante Traffic Mirroring)

Dominio 4: Identity and Access Management

Enunciado de la tarea 4.1: Diseñar, implementar y solucionar problemas de autenticación para los recursos de AWS.

Conocimientos de:

- métodos y servicios para crear y administrar identidades (por ejemplo, federación, proveedores de identidades, AWS IAM Identity Center [AWS Single
  Sign-On], Amazon Cognito)
- mecanismos de entrega de credenciales temporales y a largo plazo
- cómo solucionar problemas de autenticación (por ejemplo, mediante CloudTrail, IAM Access Advisor y el simulador de políticas de IAM)

Habilidades para:

- establecer la identidad mediante un sistema de autenticación, en función de los requisitos
- configurar la autenticación multifactor (MFA)

- determinar cuándo utilizar AWS Security Token Service (AWS STS) para emitir credenciales temporales

Enunciado de la tarea 4.2: Diseñar, implementar y solucionar problemas de autorización para los recursos de AWS.

Conocimientos de:

- diferentes políticas de IAM (por ejemplo, políticas administradas, políticas en línea, políticas basadas en identidades, políticas basadas en recursos, políticas de control de sesión)
- componentes e impacto de una política (por ejemplo, principal, acción, recurso, condición)
- cómo solucionar problemas de autorización (por ejemplo, mediante CloudTrail, IAM Access Advisor y el simulador de políticas de IAM)

Habilidades para:

- crear estrategias de control de acceso basado en atributos (ABAC) y control de acceso basado en roles (RBAC)
- evaluar los tipos de políticas de IAM para determinados requisitos y cargas de trabajo
- interpretar el efecto de una política de IAM en los entornos y las cargas de trabajo
- aplicar el principio de mínimo privilegio en un entorno
- hacer cumplir la separación adecuada de funciones
- analizar los errores de acceso o autorización para determinar la causa o el efecto
- investigar los permisos, autorizaciones o privilegios no deseados concedidos a un recurso, servicio o entidad

Dominio 5: Protección de los datos

Enunciado de la tarea 5.1: Diseñar e implementar controles que proporcionen confidencialidad e integridad a los datos en tránsito.

Conocimientos de:

- conceptos de TLS
- conceptos de VPN (por ejemplo, IPsec)

- métodos de acceso remoto seguro (por ejemplo, SSH, RDP a través de Session Manager de Systems Manager)
- conceptos de Session Manager de Systems Manager
- cómo funcionan los certificados TLS con varios servicios y recursos de red (por ejemplo, CloudFront, equilibradores de carga)

Habilidades para:

- diseñar una conectividad segura entre AWS y las redes en las instalaciones (por ejemplo, mediante el uso de Direct Connect y puertas de enlace de VPN)
- diseñar mecanismos que requieran el cifrado al conectarse a los recursos (por ejemplo, Amazon Relational Database Service, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, equilibradores de carga, Amazon Elastic File System [Amazon EFS] o Amazon API Gateway)
- exigir TLS para las llamadas API de AWS (por ejemplo, con Amazon S3)
- diseñar mecanismos para reenviar el tráfico a través de conexiones seguras (por ejemplo, mediante Systems Manager y EC2 Instance Connect)
- diseñar redes entre regiones mediante el uso de VIF privados y públicos

Enunciado de la tarea 5.2: Diseñar e implementar controles que proporcionen confidencialidad e integridad a los datos en reposo.

Conocimientos de:

- selección de la técnica de cifrado (por ejemplo, del lado del cliente, del lado del servidor, simétrica, asimétrica)
- técnicas de comprobación de la integridad (por ejemplo, algoritmos de hash, firmas digitales)
- políticas de recursos (por ejemplo, para DynamoDB, Amazon S3 y AWS Key Management Service [AWS KMS])
- políticas y roles de IAM

Habilidades para:

- diseñar políticas de recursos para restringir el acceso a los usuarios autorizados (por ejemplo, políticas de *bucket* de S3 o políticas de DynamoDB)

- diseñar mecanismos para evitar el acceso público no autorizado (por ejemplo, S3 Block Public Access, prevención de instantáneas públicas y AMI públicas)
- configurar servicios para activar el cifrado de datos en reposo (por ejemplo, Amazon S3, Amazon Relational Database Service, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon Elastic File System)
- diseñar mecanismos para proteger la integridad de los datos mediante la prevención de modificaciones (por ejemplo, mediante el uso de bloque de objetos de S3, las políticas de claves de KMS, el bloqueo de almacenes de S3 Glacier y el bloqueo de almacenes de AWS Backup)
- diseñar el cifrado en reposo mediante AWS CloudHSM para bases de datos relacionales (por ejemplo, Amazon Relational Database Service, Relational Database Service personalizado, bases de datos en instancias de EC2)
- elegir las técnicas de cifrado en función de los requisitos empresariales

Enunciado de la tarea 5.3: Diseñar e implementar controles para administrar el ciclo de vida de los datos en reposo.

Conocimientos de:

- políticas de ciclo de vida
- estándares de retención de datos

Habilidades para:

- diseñar los mecanismos de S3 Lifecycle para retener datos durante los periodos de retención requeridos (por ejemplo, bloqueo de objetos de S3, bloqueo de almacenes de S3 Glacier, políticas de S3 Lifecycle)
- diseñar la administración automática del ciclo de vida de los servicios y recursos de AWS (por ejemplo, Amazon S3, instantáneas de volúmenes de EBS, instantáneas de volumen de Relational Database Service, AMI, imágenes de contenedores, grupos de registros de CloudWatch, Amazon Data Lifecycle Manager)
- establecer cronogramas y retenciones para AWS Backup en todos los servicios de AWS

Enunciado de la tarea 5.4: Diseñar e implementar controles para proteger las credenciales, los secretos y los materiales criptográficos de claves.

Conocimientos de:

- Secrets Manager
- almacén de parámetros de Systems Manager
- uso y administración de claves simétricas y asimétricas (por ejemplo, AWS KMS)

Habilidades para:

- diseñar la administración y la rotación de los secretos para las cargas de trabajo (por ejemplo, credenciales de acceso a bases de datos, claves de API, claves de acceso de IAM, claves administradas por clientes de AWS KMS)
- diseñar políticas de claves de KMS para limitar el uso de claves a los usuarios autorizados
- establecer mecanismos para importar y eliminar el material de claves proporcionado por el cliente

Dominio 6: Administración y gobernanza de seguridad

Enunciado de la tarea 6.1: Desarrollar una estrategia para implementar y administrar las cuentas de AWS de forma centralizada.

Conocimientos de:

- estrategias para varias cuentas
- servicios administrados que permiten la administración delegada
- medidas de seguridad definidas por políticas
- prácticas recomendadas para la cuenta raíz
- roles entre cuentas

Habilidades para:

- implementar y configurar AWS Organizations
- determinar cuándo y cómo implementar AWS Control Tower (por ejemplo, qué servicios deben desactivarse para que la implementación se realice correctamente)
- implementar las *Service control policies* (SCP, políticas de control de servicios) como solución técnica para hacer cumplir una política (por

ejemplo, limitaciones en el uso de una cuenta raíz, implementación de controles en AWS Control Tower)
- administrar de forma centralizada los servicios de seguridad y agregar los hallazgos (por ejemplo, mediante la administración delegada y los agregadores de AWS Config)
- proteger las credenciales de usuario raíz de la cuenta de AWS

Enunciado de la tarea 6.2: Implementar una estrategia de implementación segura y coherente para los recursos en la nube.

Conocimientos de:
- prácticas recomendadas de implementación con infraestructura como código (IaC) (por ejemplo, fortalecimiento de plantillas de AWS CloudFormation y detección de desviaciones)
- prácticas recomendadas para el etiquetado
- administración, implementación y control de versiones centralizados de los servicios de AWS
- visibilidad y control de la infraestructura de AWS

Habilidades para:
- usar CloudFormation para implementar recursos en la nube de forma coherente y segura
- implementar y aplicar estrategias de etiquetado de múltiples cuentas
- configurar e implementar de carteras de servicios de AWS aprobados (por ejemplo, mediante AWS Service Catalog)
- organizar los recursos de AWS en diferentes grupos para su administración
- implementar Firewall Manager para hacer cumplir las políticas
- compartir recursos de forma segura entre cuentas de AWS (por ejemplo, mediante AWS Resource Access Manager [AWS RAM])

Enunciado de la tarea 6.3: Evaluar la conformidad de los recursos de AWS.

Conocimientos de:
- clasificación de datos mediante servicios de AWS
- cómo analizar, auditar y evaluar las configuraciones de los recursos de AWS (por ejemplo, mediante AWS Config)

Habilidades para:

- identificar información confidencial mediante el uso de Macie
- crear reglas de AWS Config para la detección de recursos de AWS no conformes
- recopilar y organizar pruebas mediante Security Hub y AWS Audit Manager

Enunciado de la tarea 6.4: Identificar las brechas de seguridad mediante revisiones de arquitectura y análisis de costos.

Conocimientos de:

- costo y uso de AWS para la identificación de anomalías
- estrategias para reducir las superficies de ataque
- marco de AWS Well-Architected

Habilidades para:

- identificar anomalías en función de la utilización de los recursos y las tendencias
- identificar los recursos no utilizados mediante servicios y herramientas de AWS (por ejemplo, AWS Trusted Advisor, explorador de costos de AWS)
- usar AWS Well-Architected Tool para identificar brechas de seguridad

Apéndice

Tecnologías y conceptos que pueden aparecer en el examen

En la siguiente lista, se enumeran las tecnologías y conceptos que pueden aparecer en el examen. Esta lista no es exhaustiva y está sujeta a cambios. El orden y la ubicación de los elementos de esta lista no indican su peso ni importancia relativos en el examen:

- AWS CLI
- SDK de AWS
- Consola de administración de AWS
- Acceso remoto seguro
- Administración de certificados
- Infraestructura como código (IaC)

Servicios y características de AWS dentro del alcance

Nota: La seguridad afecta a todos los servicios de AWS. Muchos servicios no aparecen en esta lista porque el servicio general está fuera del alcance, pero los aspectos de seguridad del servicio están dentro del alcance. Por ejemplo, a un candidato de este examen no se le preguntará sobre los pasos para configurar la replicación en un bucket de S3. Sin embargo, es posible que se le pregunte al candidato sobre la configuración de una política de un bucket de S3.

En la siguiente lista, se enumeran los servicios y las funciones de AWS que están dentro del alcance del examen. Esta lista no es exhaustiva y está sujeta a cambios. Las ofertas de AWS aparecen en categorías que se alinean con las funciones principales de las ofertas:

Administración y gobernanza:

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

Redes y entrega de contenido:

- Amazon VPC
  - Analizador de acceso a la red
  - Los ACL de red
  - Grupos de seguridad
  - Puntos de enlace de VPC

Seguridad, identidad y cumplimiento:

- 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

Servicios y funciones de AWS fuera de alcance del examen

En la siguiente lista, se enumeran los servicios y las funciones de AWS que están fuera del alcance del examen. Esta lista no es exhaustiva y está sujeta a cambios. Las ofertas de AWS que no tienen ninguna relación con los roles laborales objetivo para el examen se excluyen de esta lista:

Cadena de bloques:

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

Aplicaciones empresariales:

- Alexa for Business
- Amazon Chime
- SDK de Amazon Chime
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- Cadena de suministro de AWS
- AWS Wickr

- Amazon WorkDocs

Informática para usuarios finales:

- Amazon AppStream 2.0

Servicios multimedia:

- Amazon Elastic Transcoder
- Software y dispositivos de AWS Elemental
- 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

Migración y transferencia:

- Servicio de descubrimiento de aplicaciones de AWS
- AWS Application Migration Service
- AWS Database Migration Service
- Migration Evaluator
- AWS Migration Hub

- AWS Transfer Family

Tecnologías cuánticas:

- Amazon Braket

Robótica:

- AWS RoboMaker

Servicios satelitales:

- AWS Ground Station

Encuesta

¿Qué tan útil fue esta guía de examen? Infórmenos realizando nuestra encuesta