Guia do exame AWS Certified Security - Specialty (SCS-C02)

Introdução

O exame AWS Certified Security - Specialty (SCS-C02) destina-se a pessoas que desempenham uma função de segurança. O exame valida a capacidade de o candidato demonstrar, de forma eficaz, conhecimento sobre como proteger produtos e serviços da AWS.

O exame também comprova se o candidato tem:

- Compreensão das classificações de dados especializadas e dos mecanismos de proteção de dados da AWS
- Compreensão dos métodos de criptografia de dados e dos mecanismos da AWS para implementá-los
- Compreensão de protocolos seguros da Internet e dos mecanismos da AWS para implementá-los
- Conhecimento prático dos serviços e recursos de segurança da AWS para fornecer um ambiente de produção seguro
- Competência de dois anos ou mais de experiência em implantação de produção no uso dos serviços e recursos de segurança da AWS
- A capacidade de tomar decisões considerando as vantagens e desvantagens em relação ao custo, à segurança e à complexidade da implantação para atender a um conjunto de requisitos de aplicação
- Um entendimento das operações e riscos de segurança

Descrição do candidato

O candidato deve ter de três a cinco anos de experiência em projeto e implantação de soluções de segurança. Além disso, o candidato deve ter, no mínimo, dois anos de experiência prática na proteção de cargas de trabalhos da AWS.

Conhecimento da AWS recomendado

O candidato deve demonstrar conhecimento sobre:

- O modelo de responsabilidade compartilhada da AWS e sua aplicação
- Conhecimento geral dos serviços da AWS e implantação de soluções de nuvem

- Controles de segurança para ambientes e cargas de trabalho da AWS
- Estratégias de registro em log e monitoramento
- Gerenciamento de vulnerabilidades e automação de segurança
- Formas de integrar os serviços de segurança da AWS a ferramentas de terceiros
- Controles de recuperação de desastres, incluindo estratégias de backup
- Criptografia e gerenciamento de chaves
- Gerenciamento de acesso a identidade
- Retenção de dados e gerenciamento do ciclo de vida
- Como solucionar problemas de segurança
- Governança de várias contas e conformidade organizacional
- Estratégias de detecção de ameaças e resposta a incidentes

Tarefas profissionais que estão fora do escopo do candidato

A lista a seguir contém tarefas profissionais as quais não se espera que o candidato seja capaz de executar. Essa lista não é completa. Estas tarefas estão fora do escopo do exame:

- Desenvolver software em uma linguagem específica (por exemplo, Python, Java).
- Confirmar a conformidade regulatória.
- Gerenciar ciclos de vida de desenvolvimento de software.
- Projetar topologias de rede.
- Arquitetar implantações gerais de nuvem.
- Configurar serviços de armazenamento com base nos requisitos de residência de dados (por exemplo, o Regulamento Geral de Proteção de Dados [RGPD]).

Consulte no Apêndice uma lista de tecnologias e conceitos que podem aparecer no exame e uma lista de serviços e recursos da AWS dentro e fora do escopo.

Conteúdo do exame

Tipos de resposta

Existem dois tipos de perguntas no exame:

- **Múltipla escolha:** tem uma resposta correta e três respostas incorretas (distratores)

- **Múltipla resposta:** tem duas ou mais respostas corretas dentre cinco ou mais opções de resposta

Selecione uma ou mais respostas que completem melhor a afirmação ou respondam à pergunta. Pegadinhas, ou respostas incorretas, são opções de resposta que um candidato com habilidades ou conhecimentos insuficientes pode escolher. Geralmente, as pegadinhas são respostas plausíveis que correspondem à área de conteúdo.

As perguntas não respondidas são avaliadas como incorretas; não há penalidade por tentar adivinhar. O exame inclui 50 perguntas que afetam sua pontuação.

Conteúdo não avaliado

O exame inclui 15 perguntas não avaliadas que não afetam sua pontuação. A AWS coleta informações sobre o desempenho nas perguntas não avaliadas a fim de verificá-las para uso futuro como perguntas avaliadas. As perguntas não avaliadas não são identificadas no exame.

Resultados do exame

O AWS Certified Security - Specialty (SCS-C02) é um exame com uma designação de aprovação ou reprovação. O exame é avaliado de acordo com um padrão mínimo estabelecido por profissionais da AWS que seguem as práticas recomendadas e as diretrizes do setor de certificação.

Os resultados do exame são fornecidos como uma pontuação em escala de 100 a 1.000. A pontuação mínima de aprovação é de 750. A pontuação mostra como foi seu desempenho no exame como um todo e se você obteve aprovação. Os modelos de pontuação em escala ajudam a correlacionar as pontuações em várias formas de exame que podem ter níveis de dificuldade um pouco diferentes.

O relatório de pontuação pode conter uma tabela de classificações de seu desempenho em cada nível de seção. O exame usa um modelo de pontuação compensatória, o que significa que não é necessário obter uma pontuação de aprovação em cada seção. Você só precisa passar no exame geral.

Cada seção do exame tem uma ponderação específica, portanto algumas seções têm mais perguntas do que outras. A tabela de classificações contém informações gerais

que destacam seus pontos fortes e fracos. Tenha cuidado ao interpretar o feedback no nível de seção.

Resumo do conteúdo

Este guia do exame inclui as ponderações, os domínios do conteúdo e as declarações de tarefas do exame. Ele não fornece uma lista abrangente do conteúdo do exame. No entanto, um contexto adicional para cada declaração de tarefa está disponível para ajudar você a se preparar para o exame.

O exame tem os seguintes domínios do conteúdo e ponderações:

- Domínio 1: Detecção de ameaças e resposta a incidentes (14% do conteúdo pontuado)
- Domínio 2: Registro e monitoramento de segurança (18% do conteúdo pontuado)
- Domínio 3: Segurança de infraestrutura (20% do conteúdo pontuado)
- Domínio 4: Gerenciamento de identidade e acesso (16% do conteúdo pontuado)
- Domínio 5: Proteção de dados (18% do conteúdo pontuado)
- Domínio 6: Gerenciamento e governança de segurança (14% do conteúdo pontuado)

Domínio 1: Detecção de ameaças e resposta a incidentes

Declaração de tarefa 1.1: Projetar e implementar um plano de resposta a incidentes.

Conhecimento sobre:

- Práticas recomendadas da AWS para resposta a incidentes
- Incidentes na nuvem
- Funções e responsabilidades no plano de resposta a incidentes
- Formato de busca de segurança da AWS (ASFF)

Habilidades em:

- Implementar estratégias de invalidação e de troca de credenciais em resposta a comprometimentos (por exemplo, usando o AWS Identity and Access Management [IAM] e o AWS Secrets Manager)
- Isolar recursos da AWS

- Projetar e implementar manuais e runbooks para respostas a incidentes de segurança
- Implantar serviços de segurança (por exemplo, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer)
- Configurar integrações com serviços nativos da AWS e serviços de terceiros (por exemplo, usando o Amazon EventBridge e o ASFF)

Declaração de tarefa 1.2: Detectar ameaças e anomalias de segurança usando os serviços da AWS.

Conhecimento sobre:

- Serviços de segurança gerenciados pela AWS que detectam ameaças
- Técnicas de anomalia e correlação para unir dados entre serviços
- Visualizações para identificar anomalias
- Estratégias para centralizar as descobertas de segurança

Habilidades em:

- Avaliar as descobertas dos serviços de segurança (por exemplo, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer)
- Pesquisar e correlacionar ameaças à segurança nos serviços da AWS (por exemplo, usando o Detective)
- Realizar consultas para validar eventos de segurança (por exemplo, usando o Amazon Athena)
- Criar painéis e filtros de métricas para detectar atividades anômalas (por exemplo, usando o Amazon CloudWatch)

Declaração de tarefa 1.3: Responder a recursos e cargas de trabalho comprometidos.

Conhecimento sobre:

- Guia de resposta a incidentes de segurança da AWS
- Mecanismos de isolamento de recursos
- Técnicas para análise da causa raiz
- Mecanismos de captura de dados
- Análise de logs para validação de eventos

Habilidades em:

- Automatizar a correção usando serviços da AWS (por exemplo, AWS Lambda, AWS Step Functions, EventBridge, runbooks do AWS Systems Manager, Security Hub, AWS Config)
- Responder aos recursos comprometidos (por exemplo, isolando instâncias do Amazon EC2)
- Investigar e analisar para realizar a análise da causa raiz (por exemplo, usando o Detective)
- Capturar dados forenses relevantes de um recurso comprometido (por exemplo, snapshots de volume do Amazon Elastic Block Store [Amazon EBS], despejo de memória)
- Consultar logs no Amazon S3 para coletar informações contextuais relacionadas a eventos de segurança (por exemplo, usando o Athena)
- Proteger e preservar artefatos forenses (por exemplo, usando o bloqueio de objetos do S3, contas forenses isoladas, ciclo de vida do S3 e replicação do S3)
- Preparar serviços para incidentes e recuperá-los após incidentes

Domínio 2: Registro e monitoramento de segurança

Declaração de tarefa 2.1: Projetar e implementar monitoramento e alertas para abordar eventos de segurança.

Conhecimento sobre:

- Serviços da AWS que monitoram eventos e fornecem alarmes (por exemplo, CloudWatch, EventBridge)
- Serviços da AWS que automatizam alertas (por exemplo, Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub)
- Ferramentas que monitoram métricas e listas de referência (por exemplo, GuardDuty, Systems Manager)

Habilidades em:

- Analisar arquiteturas para identificar requisitos de monitoramento e origens de dados para monitoramento de segurança
- Analisar ambientes e cargas de trabalho para determinar os requisitos de monitoramento

- Projetar o monitoramento do ambiente e o monitoramento da carga de trabalho com base nos requisitos de negócios e de segurança
- Configurar ferramentas e scripts automatizados para realizar auditorias regulares (por exemplo, criando informações personalizadas no Security Hub)
- Definir as métricas e os limites que geram alertas

Declaração de tarefa 2.2: Solucionar problemas de monitoramento e alertas de segurança.

Conhecimento sobre:

- Configuração de serviços de monitoramento (por exemplo, Security Hub)
- Dados relevantes que indicam eventos de segurança

Habilidades em:

- Analisar a funcionalidade do serviço, as permissões e a configuração dos recursos após um evento que não forneceu visibilidade ou alerta
- Analisar e corrigir a configuração de um aplicativo personalizado que não está relatando as respectivas estatísticas
- Avaliar os serviços de registro e monitoramento para alinhamento com os requisitos de segurança

Declaração de tarefa 2.3: Projetar e implementar uma solução de registro em log.

Conhecimento sobre:

- Serviços e recursos da AWS que fornecem funcionalidades de registro (por exemplo, logs de fluxo da VPC, logs de DNS, AWS CloudTrail, Amazon CloudWatch Logs)
- Atributos das funcionalidades de registro (por exemplo, níveis de log, tipo, verbosidade)
- Destinos de log e gerenciamento do ciclo de vida (por exemplo, período de retenção)

Habilidades em:

- Configurar o registro para serviços e aplicativos
- Identificar requisitos de registro e origens para ingestão de logs

- Implementar o armazenamento de logs e o gerenciamento do ciclo de vida de acordo com os requisitos organizacionais e as práticas recomendadas da AWS

Declaração de tarefa 2.4: Solucionar problemas de registros em log.

Conhecimento sobre:

- Recursos e casos de uso de serviços da AWS que fornecem origens dos dados (por exemplo, nível de log, tipo, verbosidade, cadência, pontualidade, imutabilidade)
- Serviços e recursos da AWS que fornecem funcionalidades de registro (por exemplo, logs de fluxo da VPC, logs de DNS, CloudTrail, CloudWatch Logs)
- Permissões de acesso necessárias para o registro

Habilidades em:

- Identificar a configuração incorreta e determinar as etapas de correção para permissões de acesso ausentes que são necessárias para o registro (por exemplo, gerenciar permissões de leitura/gravação, permissões de bucket do S3, acesso público e integridade)
- Determinar a causa da falta de logs e executar as etapas de correção

Declaração de tarefa 2.5: Projetar uma solução de análise de logs.

Conhecimento sobre:

- Serviços e ferramentas para analisar logs capturados (por exemplo, Athena, filtro do CloudWatch Logs)
- Recursos de análise de logs dos serviços da AWS (por exemplo, CloudWatch Logs Insights, CloudTrail Insights, Security Hub Insights)
- Formato e componentes do log (por exemplo, logs do CloudTrail)

Habilidades em:

- Identificar padrões em logs para indicar anomalias e ameaças conhecidas
- Normalizar, analisar e correlacionar logs

Domínio 3: Segurança de infraestrutura

Declaração de tarefa 3.1: Projetar e implementar controles de segurança para serviços de borda.

Conhecimento sobre:

- Recursos de segurança em serviços de borda (por exemplo, AWS WAF, balanceadores de carga, Amazon Route 53, Amazon CloudFront, AWS Shield)
- Ataques, ameaças e explorações comuns (por exemplo, Top 10 do Open Web Application Security Project [OWASP], DDoS)
- Arquitetura de aplicativos web em camadas

Habilidades em:

- Definir estratégias de segurança de borda para casos de uso comuns (por exemplo, site público, aplicativo sem servidor, back-end de aplicativo móvel)
- Selecionar serviços de borda apropriados com base nas ameaças e ataques previstos (por exemplo, Top 10 do OWASP, DDoS)
- Selecionar proteções apropriadas com base nas vulnerabilidades e nos riscos previstos (por exemplo, software, aplicativos e bibliotecas vulneráveis)
- Definir camadas de defesa combinando serviços de segurança de borda (por exemplo, CloudFront com AWS WAF e balanceadores de carga)
- Aplicar restrições na borda com base em vários critérios (por exemplo, geografia, geolocalização, limite de taxa)
- Ativar logs, métricas e monitoramento de serviços de borda para indicar ataques

Declaração de tarefa 3.2: Projetar e implementar controles de segurança de rede.

Conhecimento sobre:

- Mecanismos de segurança da VPC (por exemplo, grupos de segurança, ACLs de rede, AWS Network Firewall)
- Conectividade entre VPC (por exemplo, AWS Transit Gateway, endpoints de VPC)

- Origens de telemetria de segurança (por exemplo, espelhamento de tráfego, logs de fluxo da VPC)
- Tecnologia, terminologia e uso de VPN
- Opções de conectividade on-premises (por exemplo, AWS VPN, AWS Direct Connect)

Habilidades em:

- Implementar a segmentação de rede com base em requisitos de segurança (por exemplo, sub-redes públicas, sub-redes privadas, VPCs sigilosas, conectividade on-premises)
- Projetar controles de rede para permitir ou impedir o tráfego de rede conforme necessário (por exemplo, usando grupos de segurança, ACLs de rede e firewall de rede)
- Projetar fluxos de rede para manter os dados fora da Internet pública (por exemplo, usando Transit Gateway, endpoints de VPC e Lambda em VPCs)
- Determinar quais origens de telemetria monitorar com base no projeto, nas ameaças e nos ataques da rede (por exemplo, logs do balanceador de carga, logs de fluxo da VPC, espelhamento de tráfego)
- Determinar os requisitos de redundância e de carga de trabalho de segurança para comunicação entre ambientes on-premises e a nuvem AWS (por exemplo, usando AWS VPN, AWS VPN via Direct Connect e MACsec)
- Identificar e remover o acesso desnecessário à rede
- Gerenciar configurações de rede conforme os requisitos mudam (por exemplo, usando o AWS Firewall Manager)

Declaração de tarefa 3.3: Projetar e implementar controles de segurança para cargas de trabalho de computação.

Conhecimento sobre:

- Provisionamento e manutenção de instâncias do EC2 (por exemplo, aplicação de patches, inspeção, criação de snapshots e AMIs, uso do EC2 Image Builder)
- Perfis de instância do IAM e perfis de serviço do IAM
- Serviços que verificam vulnerabilidades em cargas de trabalho de computação (por exemplo, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR])

- Segurança baseada em host (por exemplo, firewalls, proteção)

Habilidades em:

- Criar AMIs reforçadas do EC2
- Aplicar perfis de instância e perfis de serviço conforme apropriado para autorizar cargas de trabalho de computação
- Verificar instâncias do EC2 e imagens de contêineres em busca de vulnerabilidades conhecidas
- Aplicar patches em uma frota de instâncias do EC2 ou imagens de contêineres
- Ativar mecanismos de segurança baseados em host (por exemplo, firewalls baseados em host)
- Analisar as descobertas do Amazon Inspector e determinar as técnicas de mitigação apropriadas
- Transmitir segredos e credenciais com segurança para cargas de trabalho de computação

Declaração de tarefa 3.4: Solucionar problemas de segurança de rede.

Conhecimento sobre:

- Como analisar a acessibilidade (por exemplo, usando o VPC Reachability Analyzer e o Amazon Inspector)
- Conceitos fundamentais de redes TCP/IP (por exemplo, UDP comparado com TCP, portas, modelo Open Systems Interconnection [OSI], utilitários do sistema operacional de rede)
- Como ler origens de log relevantes (por exemplo, logs do Route 53, logs do AWS WAF, logs de fluxo da VPC)

Habilidades em:

- Identificar, interpretar e priorizar problemas na conectividade de rede (por exemplo, usando o Amazon Inspector Network Reachability)
- Determinar soluções para produzir o comportamento de rede desejado
- Analisar origens de log para identificar problemas
- Capturar amostras de tráfego para análise de problemas (por exemplo, usando o espelhamento de tráfego)

Domínio 4: Identity and Access Management

Declaração de tarefa 4.1: Projetar, implementar e solucionar problemas de autenticação de recursos da AWS.

Conhecimento sobre:

- Métodos e serviços para criar e gerenciar identidades (por exemplo, federação, provedores de identidade, AWS IAM Identity Center [AWS Single Sign-On], Amazon Cognito)
- Mecanismos de credenciamento temporários e de longo prazo
- Como solucionar problemas de autenticação (por exemplo, usando o CloudTrail, o IAM Access Advisor e o simulador de políticas do IAM)

Habilidades em:

- Estabelecer identidade por meio de um sistema de autenticação, com base nos requisitos
- Habilitar a autenticação com multifator (MFA)
- Determinar quando usar o AWS Security Token Service (AWS STS) para emitir credenciais temporárias

Declaração de tarefa 4.2: Projetar, implementar e solucionar problemas de autorização de recursos da AWS.

Conhecimento sobre:

- Políticas diferentes do IAM (por exemplo, políticas gerenciadas, políticas em linha, políticas baseadas em identidade, políticas baseadas em recursos, políticas de controle de sessão)
- Componentes e impacto de uma política (por exemplo, principal, ação, recurso, condição)
- Como solucionar problemas de autorização (por exemplo, usando o CloudTrail, o IAM Access Advisor e o simulador de políticas do IAM)

Habilidades em:

- Construir estratégias de controle de acesso baseado em atributos (ABAC) e controle de acesso baseado em perfis (RBAC)
- Avaliar os tipos de políticas do IAM para determinados requisitos e cargas de trabalho

- Interpretar o efeito de uma política do IAM em ambientes e cargas de trabalho
- Aplicar o princípio de menor privilégio em um ambiente
- Impor a separação adequada de deveres
- Analisar erros de acesso ou de autorização para determinar causa ou efeito
- Investigar permissões, autorizações ou privilégios não intencionais concedidos a um recurso, um serviço ou uma entidade

Domínio 5: Proteção de dados

Declaração de tarefa 5.1: Projetar e implementar controles que promovam confidencialidade e integridade aos dados em trânsito.

Conhecimento sobre:

- Conceitos de TLS
- Conceitos de VPN (por exemplo, IPsec)
- Métodos de acesso remoto seguro (por exemplo, SSH, RDP sobre o gerenciador de sessões do Systems Manager)
- Conceitos do gerenciador de sessões do Systems Manager
- Como os certificados TLS funcionam com vários serviços e recursos de rede (por exemplo, CloudFront, balanceadores de carga)

Habilidades em:

- Projetar conectividade segura entre a AWS e redes on-premises (por exemplo, usando o Direct Connect e gateways da VPN)
- Projetar mecanismos para exigir criptografia ao se conectar a recursos (por exemplo, Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, balanceadores de carga, Amazon Elastic File System [Amazon EFS], Amazon API Gateway)
- Exigir TLS para chamadas de API da AWS (por exemplo, com o Amazon S3)
- Projetar mecanismos para encaminhar tráfego por conexões seguras (por exemplo, usando o Systems Manager e o EC2 Instance Connect)
- Projetar redes entre regiões usando VIFs privadas e VIFs públicas

Declaração de tarefa 5.2: Projetar e implementar controles que promovam confidencialidade e integridade para dados em repouso.

Conhecimento sobre:

- Seleção da técnicas de criptografia (por exemplo, do lado do cliente, do lado do servidor, simétrica, assimétrica)
- Técnicas de verificação de integridade (por exemplo, algoritmos de hashing, assinaturas digitais)
- Políticas de recursos (por exemplo, para DynamoDB, Amazon S3 e AWS Key Management Service [AWS KMS])
- Perfis e políticas do IAM

Habilidades em:

- Projetar políticas de recursos para restringir o acesso a usuários autorizados (por exemplo, políticas de bucket do S3, políticas do DynamoDB)
- Projetar mecanismos para impedir o acesso público não autorizado (por exemplo, bloqueio de acesso público do S3, prevenção de snapshots públicos e AMIs públicas)
- Configurar serviços para ativar a criptografia de dados em repouso (por exemplo, Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS)
- Projetar mecanismos para proteger a integridade dos dados evitando modificações (por exemplo, usando o bloqueio de objetos do S3, as políticas de chave do KMS, o Vault Lock do S3 Glacier e o Vault Lock do AWS Backup)
- Projetar a criptografia em repouso usando o AWS CloudHSM para bancos de dados relacionais (por exemplo, Amazon RDS, RDS Custom, bancos de dados em instâncias do EC2)
- Escolher técnicas de criptografia com base nos requisitos de negócios

Declaração de tarefa 5.3: Projetar e implementar controles para gerenciar o ciclo de vida dos dados em repouso.

Conhecimento sobre:

- Políticas de ciclo de vida
- Padrões de retenção de dados

Habilidades em:

- Projetar mecanismos de ciclo de vida do S3 para reter dados durante os períodos de retenção necessários (por exemplo, bloqueio de objetos do S3, Vault Lock do S3 Glacier, política de ciclo de vida do S3)
- Projetar o gerenciamento automático do ciclo de vida de serviços e recursos da AWS (por exemplo, Amazon S3, snapshots de volume do EBS, snapshots de volume do RDS, AMIs, imagens de contêineres, grupos de logs do CloudWatch, Amazon Data Lifecycle Manager)
- Estabelecer cronogramas e retenção para o AWS Backup nos serviços da AWS

Declaração de tarefa 5.4: Projetar e implementar controles para proteger credenciais, segredos e materiais de chaves criptográficas.

Conhecimento sobre:

- Secrets Manager
- Systems Manager Parameter Store
- Uso e gerenciamento de chaves simétricas e assimétricas (por exemplo, AWS KMS)

Habilidades em:

- Projetar o gerenciamento e a troca de segredos para cargas de trabalho (por exemplo, credenciais de acesso ao banco de dados, chaves de API, chaves de acesso do IAM, chaves gerenciadas pelo cliente do AWS KMS)
- Projetar políticas de chave do KMS para limitar o uso da chave a usuários autorizados
- Estabelecer mecanismos para importar e remover material de chave fornecido pelo cliente

Domínio 6: Gerenciamento e governança de segurança

Declaração de tarefa 6.1: Desenvolver uma estratégia para implantar e gerenciar de maneira centralizada as contas da AWS.

Conhecimento sobre:

- Estratégias de várias contas
- Serviços gerenciados que permitem a administração delegada

- Proteções definidas por políticas
- Práticas recomendadas da conta-raiz
- Perfis entre contas

Habilidades em:

- Implantar e configurar o AWS Organizations
- Determinar quando e como implantar o AWS Control Tower (por exemplo, quais serviços devem ser desativados para uma implantação bem-sucedida)
- Implementar SCPs como uma solução técnica para aplicar uma política (por exemplo, limitações no uso de uma conta raiz, implementação de controles no AWS Control Tower)
- Gerenciar de forma centralizada os serviços de segurança e agregar descobertas (por exemplo, usando administração delegada e agregadores do AWS Config)
- Proteger as credenciais do usuário-raiz da conta da AWS

Declaração de tarefa 6.2: Implementar uma estratégia de implantação segura e consistente para recursos de nuvem.

Conhecimento sobre:

- Práticas recomendadas de implantação com infraestrutura como código (IaC) (por exemplo, fortalecimento de modelos do AWS CloudFormation e detecção de desvios)
- Práticas recomendadas para marcação
- Gerenciamento, implantação e versionamento centralizados dos serviços da AWS
- Visibilidade e controle sobre a infraestrutura da AWS

Habilidades em:

- Usar o CloudFormation para implantar recursos de nuvem de forma consistente e segura
- Implementar e aplicar estratégias de marcação de várias contas
- Configurar e implantar portfólios de serviços aprovados da AWS (por exemplo, usando o AWS Service Catalog)
- Organizar os recursos da AWS em diferentes grupos para gerenciamento
- Implantar o Firewall Manager para aplicar políticas

- Compartilhar com segurança recursos entre contas da AWS (por exemplo, usando o AWS Resource Access Manager [AWS RAM])

Declaração de tarefa 6.3: Avaliar a conformidade dos recursos da AWS.

Conhecimento sobre:

- Classificação de dados usando os serviços da AWS
- Como analisar, auditar e avaliar as configurações dos recursos da AWS (por exemplo, usando o AWS Config)

Habilidades em:

- Identificar dados sigilosos usando o Macie
- Criar regras do AWS Config para detecção de recursos da AWS que não estão em conformidade
- Coletar e organizar evidências usando o Security Hub e o AWS Audit Manager

Declaração de tarefa 6.4: Identificar as falhas de segurança por meio de avaliações de arquitetura e análise de custos.

Conhecimento sobre:

- Custo e uso da AWS para identificação de anomalias
- Estratégias para reduzir as superfícies de ataque
- AWS Well-Architected Framework

Habilidades em:

- Identificar anomalias com base na utilização de recursos e tendências
- Identificar recursos não utilizados usando serviços e ferramentas da AWS (por exemplo, AWS Trusted Advisor, AWS Cost Explorer)
- Usar a ferramenta do AWS Well-Architected para identificar falhas de segurança

Apêndice

Tecnologias e conceitos que podem aparecer no exame

A lista a seguir contém tecnologias e conceitos que podem aparecer no exame. Essa lista não é completa e está sujeita a alterações. A ordem e a posição dos itens nessa lista não indicam seu peso relativo ou importância no exame:

- AWS CLI
- SDKs da AWS
- Console de gerenciamento da AWS
- Acesso remoto seguro
- Gerenciamento de certificados
- Infraestrutura como código (IaC)

Recursos e produtos da AWS no escopo

Nota: a segurança afeta todos os serviços da AWS. Muitos serviços não aparecem nessa lista porque o serviço geral está fora do escopo, mas os aspectos de segurança do serviço estão no escopo. Por exemplo, um candidato para esse exame não seria questionado sobre as etapas para configurar a replicação de um bucket do S3. No entanto, o candidato pode ser questionado sobre a configuração de uma política de bucket do S3.

A lista a seguir contém os serviços e recursos da AWS que estão no escopo do exame. Essa lista não é completa e está sujeita a alterações. As ofertas da AWS aparecem em categorias que se alinham às funções principais das ofertas:

Gerenciamento e governança:

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

Redes e entrega de conteúdo:

- Amazon VPC
  - Network Access Analyzer
  - ACLs de rede
  - Grupos de segurança
  - Endpoints da VPC

Segurança, identidade e conformidade:

- 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

Recursos e serviços da AWS fora do escopo

A lista a seguir contém serviços e recursos da AWS que estão fora do escopo do exame. Essa lista não é completa e está sujeita a alterações. As ofertas da AWS que não estão totalmente relacionadas às funções de trabalho desejadas para o exame foram excluídas dessa lista:

Blockchain:

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

Aplicações empresariais:

- Alexa for Business
- Amazon Chime
- SDK do Amazon Chime
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- Cadeia de Suprimentos AWS
- AWS Wickr
- Amazon WorkDocs

Computação de usuário final:

- Amazon AppStream 2.0

Serviços de mídia:

- Amazon Elastic Transcoder
- Dispositivos e software do 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

Migração e transferência:

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

Tecnologias quânticas:

- Amazon Braket

Robótica:

- AWS RoboMaker

Satélite:

- AWS Ground Station

Pesquisa

Este guia do exame foi útil? Informe-nos respondendo à nossa pesquisa