Guia do exame AWS Certified Security - Specialty (SCS-C03)

Introdução

O exame AWS Certified Security - Specialty (SCS-C03) é destinado a profissionais responsáveis por proteger soluções de nuvem. O exame valida a capacidade de o candidato demonstrar, de forma eficaz, conhecimento sobre como proteger produtos e serviços da AWS.

O exame também valida a capacidade do candidato de concluir as seguintes tarefas:

- Aplicar classificações especializadas de dados e mecanismos de proteção de dados da AWS.
- Implementar métodos de criptografia de dados e mecanismos de criptografia da AWS.
- Implementar mecanismos da AWS para seguir protocolos de internet seguros.
- Usar os serviços e recursos de segurança da AWS para garantir ambientes de produção seguros.
- Tomar decisões que equilibrem custo, segurança e complexidade de implantação para atender a um conjunto de requisitos de aplicações.
- Entender as operações de segurança e os riscos envolvidos.

Descrição do candidato

O candidato deve ter o equivalente a três a cinco anos de experiência na proteção de soluções de nuvem.

Conhecimento da AWS recomendado

O candidato deve ter o seguinte conhecimento da AWS:

- O modelo de responsabilidade compartilhada da AWS e sua aplicação
- Gerenciamento de identidades em grande escala
- Governança de várias contas
- Gerenciamento dos riscos da cadeia de fornecimento de software
- Estratégias de prevenção e resposta a incidentes de segurança
- Gerenciamento de vulnerabilidades na nuvem
- Desenvolvimento de regras de firewall em escala para as camadas três a sete

- Análise da causa raiz de incidentes
- Experiência na resposta a auditorias
- Estratégias de registro em log e monitoramento
- Metodologias de criptografia de dados, tanto em repouso quanto em trânsito
- Controles de recuperação de desastres, incluindo estratégias de backup

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:

- Criar algoritmos criptográficos
- Analisar o tráfego no nível do pacote
- Arquitetar implantações gerais na nuvem
- Gerenciar recursos de computação para usuários finais
- Treinar modelos de machine learning

Consulte no Apêndice as listas de serviços e recursos da AWS que estão incluídos e excluídos do escopo do exame.

Conteúdo do exame

Tipos de respostas

O exame inclui um ou mais dos seguintes tipos de perguntas:

- **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
- **Ordenação:** tem uma lista de três a cinco respostas para concluir uma tarefa específica. Você deve selecionar as respostas certas e colocá-las na ordem correta para receber crédito pela pergunta.
- **Correspondência:** tem uma lista de respostas que correspondem a uma lista de três a sete questões. Você deve correlacionar todos os pares corretamente para receber crédito pela pergunta.

As perguntas não respondidas são classificadas como incorretas. Não há penalidade por tentar adivinhar a resposta. O exame inclui 50 perguntas que afetam sua pontuação[1].

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-C03) 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.

[1] Não se aplica à versão beta do exame. É possível encontrar mais informações sobre os exames beta em geral no site do AWS Certification.

Resumo do conteúdo

Este guia do exame inclui as ponderações, os domínios do conteúdo e as tarefas do exame. Este guia não fornece uma lista abrangente do conteúdo do exame.

O exame tem os seguintes domínios do conteúdo e ponderações:

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

Domínio do conteúdo 1: Detecção

Tarefa 1.1: Projetar e implementar soluções de monitoramento e alertas para uma organização ou conta da AWS.

Habilidade 1.1.1: Analisar workloads para determinar os requisitos de monitoramento.
Habilidade 1.1.2: Projetar e implementar estratégias de monitoramento de workloads (por exemplo, configurar verificações de integridade de recursos).
Habilidade 1.1.3: Agregar eventos de segurança e monitoramento.
Habilidade 1.1.4: Criar métricas, alertas e painéis para detectar dados e eventos anômalos (por exemplo, Amazon GuardDuty, Amazon Security Lake, AWS Security Hub, Amazon Macie).
Habilidade 1.1.5: Criar e gerenciar automações para realizar avaliações e investigações regulares (por exemplo, implantar pacotes de conformidade do AWS Config, o Security Hub, o Gerenciador de Estados do AWS Systems Manager).

Tarefa 1.2: Projetar e implementar soluções de registro em log.

Habilidade 1.2.1: Identificar as origens para ingestão e armazenamento de logs com base nos requisitos.

Habilidade 1.2.2: Configurar o registro em log para serviços e aplicações da AWS (por exemplo, configurar uma trilha do AWS CloudTrail para uma organização, criar uma conta de registro em log dedicada do Amazon CloudWatch, configurar o agente do Amazon CloudWatch Logs).
Habilidade 1.2.3: Implementar armazenamento de logs e data lakes de logs (por exemplo, Security Lake) e integrá-los a ferramentas de segurança de terceiros.
Habilidade 1.2.4: Usar os serviços da AWS para analisar logs (por exemplo, CloudWatch Logs Insights, Amazon Athena, descobertas do Security Hub).
Habilidade 1.2.5: Usar os serviços da AWS para normalizar, analisar e correlacionar logs (por exemplo, Amazon OpenSearch Service, AWS Lambda, Amazon Managed Grafana).
Habilidade 1.2.6: Determinar e configurar as origens de log apropriadas com base no design da rede, nas ameaças e nos ataques (por exemplo, logs de fluxo da VPC, logs de fluxo do gateway de trânsito, logs do Amazon Route 53 Resolver).

Tarefa 1.3: Solucionar problemas relacionados a soluções de registro em log, alertas e monitoramento da segurança.

Habilidade 1.3.1: Analisar a funcionalidade, as permissões e a configuração dos recursos (por exemplo, registro em log de funções do Lambda, registro em log do Amazon API Gateway, verificações de integridade, registro em log do Amazon CloudFront).
Habilidade 1.3.2: Corrigir configurações incorretas de recursos (por exemplo, solucionar problemas nas configurações do agente do CloudWatch, solucionar problemas de logs ausentes).

Domínio do conteúdo 2: Resposta a incidentes

Tarefa 2.1: Projetar e testar um plano de resposta a incidentes.

Habilidade 2.1.1: Projetar e implementar planos de resposta e runbooks para responder a incidentes de segurança (por exemplo, Systems Manager OpsCenter, cadernos do Amazon SageMaker IA).
Habilidade 2.1.2: Utilizar os recursos e as capacidades dos serviços da AWS para configurar os serviços de modo a estarem preparados para incidentes (por exemplo, provisionar acesso, implantar ferramentas de segurança, minimizar o raio de alcance do impacto e configurar proteções do AWS Shield Avançado).

Habilidade 2.1.3: Recomendar procedimentos para testar e validar a eficácia de um plano de resposta a incidentes (por exemplo, AWS Fault Injection Service, Hub de Resiliência da AWS).
Habilidade 2.1.4: Utilizar os serviços da AWS para corrigir incidentes automaticamente (por exemplo, Systems Manager, Automated Forensics Orchestrator para Amazon EC2, AWS Step Functions, Amazon Application Recovery Controller, funções do Lambda).

Tarefa 2.2: Responder a eventos de segurança.

Habilidade 2.2.1: Capturar e armazenar logs relevantes do sistema e da aplicação como artefatos forenses.
Habilidade 2.2.2: Pesquisar e correlacionar logs de eventos de segurança em aplicações e serviços da AWS.
Habilidade 2.2.3: Validar as descobertas dos serviços de segurança da AWS para avaliar o escopo e o impacto de um evento.
Habilidade 2.2.4: Responder aos recursos afetados contendo e erradicando ameaças e recuperar recursos (por exemplo, com a implementação de controles de contenção de rede e restauração de backups).
Habilidade 2.2.5: Descrever os métodos para conduzir a análise da causa raiz (por exemplo, Amazon Detective).

Domínio do conteúdo 3: Segurança de infraestrutura

Tarefa 3.1: Projetar, implementar e solucionar problemas de controles de segurança para serviços de borda da rede.

Habilidade 3.1.1: Definir e selecionar estratégias de segurança de borda com base nas ameaças e ataques previstos.
Habilidade 3.1.2: Implementar a proteção apropriada da borda da rede (por exemplo, cabeçalhos do CloudFront, AWS WAF, políticas do AWS IoT, proteção contra as ameaças indicadas no Top 10 do OWASP, compartilhamento de recursos de origem cruzada [CORS] do Amazon S3, Shield Avançado).
Habilidade 3.1.3: Projetar e implementar controles de borda e regras da AWS com base nos requisitos (por exemplo, geografia, geolocalização, limitação de taxa, impressão digital do cliente).

Habilidade 3.1.4: Configurar integrações com serviços de borda da AWS e serviços de terceiros (por exemplo, ingerir dados no formato Open Cybersecurity Schema Framework [OCSF], usando regras WAF de terceiros).

Tarefa 3.2: Projetar, implementar e solucionar problemas de controles de segurança para workloads de computação.

Habilidade 3.2.1: Projetar e implementar AMIs reforçadas do Amazon EC2 e imagens de contêiner para proteger workloads de computação e incorporar controles de segurança (por exemplo, Systems Manager, EC2 Image Builder).
Habilidade 3.2.2: Aplicar perfis de instância, perfis de serviço e perfis de execução de forma adequada para autorizar workloads de computação.
Habilidade 3.2.3: Verificar os recursos de computação em busca de vulnerabilidades conhecidas (por exemplo, verificar imagens de contêineres e funções do Lambda usando o Amazon Inspector, monitorar os runtimes de computação usando o GuardDuty).
Habilidade 3.2.4: Implantar patches em recursos de computação para manter ambientes seguros e em conformidade, automatizando os processos de atualização e integrando a validação contínua (por exemplo, Gerenciador de Patches do Systems Manager, Amazon Inspector).
Habilidade 3.2.5: Configurar o acesso administrativo seguro aos recursos de computação (por exemplo, Systems Manager Session Manager, EC2 Instance Connect).
Habilidade 3.2.6: Configurar ferramentas de segurança para descobrir e corrigir vulnerabilidades em um pipeline (por exemplo, Amazon Q Developer, Amazon CodeGuru Security).
Habilidade 3.2.7: Implementar proteções e barreiras de proteção para aplicações de IA generativa (por exemplo, aplicar as proteções do Top 10 de IA generativa do OWASP para aplicações de LLM).

Tarefa 3.3: Projetar e solucionar problemas de controles de segurança de rede.

Habilidade 3.3.1: Projetar e solucionar problemas de controles de rede apropriados para permitir ou impedir o tráfego de rede conforme necessário (por exemplo, grupos de segurança, ACLs de rede, AWS Network Firewall).
Habilidade 3.3.2: Criar conectividade segura entre redes híbridas e de várias nuvens (por exemplo, AWS Site-to-Site VPN, AWS Direct Connect, MAC Security [MACsec]).

Habilidade 3.3.3: Determinar e configurar os requisitos de workload de segurança para comunicação entre ambientes híbridos e a AWS (por exemplo, usando o Acesso Verificado pela AWS).
Habilidade 3.3.4: Projetar a segmentação da rede com base nos requisitos de segurança (por exemplo, proteções de tráfego norte/sul e leste/oeste, sub-redes isoladas).
Habilidade 3.3.5: Identificar o acesso desnecessário à rede (por exemplo, Acesso Verificado pela AWS, Network Access Analyzer, descobertas de acessibilidade de rede do Amazon Inspector).

Domínio do conteúdo 4: Gerenciamento de identidade e acesso

Tarefa 4.1: Projetar, implementar e solucionar problemas de estratégias de autenticação.

Habilidade 4.1.1: Projetar e estabelecer soluções de identidade para autenticação humana, de aplicações e de sistemas (por exemplo, Centro de Identidade do AWS IAM, Amazon Cognito, autenticação multifator [MFA], integração com provedor de identidades [IdP]).
Habilidade 4.1.2: Configurar mecanismos para emitir credenciais temporárias (por exemplo, AWS Security Token Service [AWS STS], URLs predefinidos do Amazon S3).
Habilidade 4.1.3: Solucionar problemas de autenticação (por exemplo, CloudTrail, Amazon Cognito, conjuntos de permissões do Centro de Identidade do IAM, AWS Directory Service).

Tarefa 4.2: Projetar, implementar e solucionar problemas de estratégias de autorização.

Habilidade 4.2.1: Projetar e avaliar controles de autorização para acesso humano, de aplicações e de sistemas (por exemplo, Amazon Verified Permissions, caminhos do IAM, IAM Roles Anywhere, políticas de recursos para acesso entre contas, políticas de confiança de perfis do IAM).
Habilidade 4.2.2: Criar estratégias de controle de acesso baseado em atributos (ABAC) e controle de acesso baseado em perfis (RBAC) (por exemplo, configurar o acesso a recursos com base em tags ou atributos).
Habilidade 4.2.3: Criar, interpretar e implementar políticas do IAM seguindo o princípio de menor privilégio (por exemplo, limites de permissão, políticas de sessão).
Habilidade 4.2.4: Analisar falhas de autorização para determinar causas ou efeitos (por exemplo, Simulador de políticas do IAM, IAM Access Analyzer).

Habilidade 4.2.5: Investigar e corrigir permissões, autorizações ou privilégios não intencionais concedidos a um recurso, um serviço ou uma entidade (por exemplo, IAM Access Analyzer).

Domínio do conteúdo 5: Proteção de dados

Tarefa 5.1: Projetar e implementar controles para dados em trânsito.

Habilidade 5.1.1: Projetar e configurar mecanismos que exijam criptografia ao se conectar aos recursos (por exemplo, configurar as políticas de segurança do Elastic Load Balancing [ELB], aplicar configurações de TLS).
Habilidade 5.1.2: Projetar e configurar mecanismos para acesso seguro e privado aos recursos (por exemplo, AWS PrivateLink, endpoints da VPC, AWS Client VPN, Acesso Verificado pela AWS).
Habilidade 5.1.3: Projetar e configurar a criptografia entre recursos em trânsito (por exemplo, configurações de criptografia entre nós para Amazon EMR, Amazon Elastic Kubernetes Service [Amazon EKS], SageMaker IA, criptografia Nitro).

Tarefa 5.2: Projetar e implementar controles para dados em repouso.

Habilidade 5.2.1: Projetar, implementar e configurar a criptografia de dados em repouso com base em requisitos específicos (por exemplo, selecionar o serviço de chave de criptografia apropriado, como o AWS CloudHSM ou o AWS Key Management Service [AWS KMS], ou selecionar o tipo de criptografia apropriado, como criptografia do lado do cliente ou criptografia do lado do servidor).
Habilidade 5.2.2: Projetar e configurar mecanismos para proteger a integridade dos dados (por exemplo, Bloqueio de objetos do S3, S3 Glacier Vault Lock, versionamento, assinatura de código digital, validação de arquivos).
Habilidade 5.2.3: Criar soluções automáticas de gerenciamento e retenção do ciclo de vida para dados (por exemplo, políticas de ciclo de vida do S3, Bloqueio de objetos do S3, políticas de ciclo de vida do Amazon Elastic File System [Amazon EFS], políticas de backup do Amazon FSx para Lustre).
Habilidade 5.2.4: Projetar e configurar soluções seguras de replicação e backup de dados (por exemplo, Amazon Data Lifecycle Manager, AWS Backup, proteção contra ransomware, AWS DataSync).

Tarefa 5.3: Projetar e implementar controles para proteger dados confidenciais, segredos e materiais de chaves criptográficas.

Habilidade 5.3.1: Gerenciamento de design e alternância de credenciais e segredos (por exemplo, AWS Secrets Manager).
Habilidade 5.3.2: Gerenciar e usar material de chave importado (por exemplo, gerenciar e alternar o material de chave importado, gerenciar e configurar armazenamentos de chaves externos).
Habilidade 5.3.3: Descrever as diferenças entre o material de chave importado e o material de chave gerado pela AWS.
Habilidade 5.3.4: Mascarar dados sensíveis (por exemplo, políticas de proteção de dados do CloudWatch Logs, proteção de dados de mensagens do Amazon Simple Notification Service [Amazon SNS]).
Habilidade 5.3.5: Criar e gerenciar chaves de criptografia e certificados em uma única Região AWS ou em várias regiões (por exemplo, chaves do AWS KMS gerenciadas pelo cliente do AWS KMS, AWS Private Certificate Authority).

Domínio do conteúdo 6: Governança e fundamentos de segurança

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

Habilidade 6.1.1: Implantar e configurar organizações usando o AWS Organizations.
Habilidade 6.1.2: Implementar e gerenciar o AWS Control Tower em ambientes novos e existentes e implantar controles opcionais e personalizados.
Habilidade 6.1.3: Implementar políticas organizacionais para gerenciar permissões (por exemplo, SCPs, RCPs, políticas de cancelamento de serviços de IA, políticas declarativas).
Habilidade 6.1.4: Gerenciar centralmente os serviços de segurança (por exemplo, contas de administrador delegado).
Habilidade 6.1.5: Gerenciar as credenciais do usuário-raiz da conta da AWS (por exemplo, centralizar o acesso-raiz para contas de membros, gerenciar a MFA, projetar procedimentos de emergência).

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

Habilidade 6.2.1: Usar a infraestrutura como código (IaC) para implantar recursos de nuvem de forma consistente e segura em todas as contas (por exemplo, conjuntos de pilhas do CloudFormation, ferramentas de IaC de terceiros, CloudFormation Guard, cfn-lint).
Habilidade 6.2.2: Usar tags para organizar os recursos da AWS em grupos para gerenciamento (por exemplo, agrupar por departamento, centro de custos, ambiente).
Habilidade 6.2.3: Implantar e aplicar políticas e configurações por uma fonte central (por exemplo, o AWS Firewall Manager).
Habilidade 6.2.4: Compartilhar recursos com segurança entre contas da AWS (por exemplo, AWS Service Catalog, AWS Resource Access Manager [AWS RAM]).

Tarefa 6.3: Avaliar a conformidade dos recursos da AWS.

Habilidade 6.3.1: Criar ou ativar regras para detectar e corrigir recursos da AWS que não estão em conformidade e enviar notificações (por exemplo, usando o AWS Config para agregar alertas e corrigir recursos que não estão em conformidade, Security Hub).
Habilidade 6.3.2: Usar os serviços de auditoria da AWS para coletar e organizar evidências (por exemplo, AWS Audit Manager, AWS Artifact).
Habilidade 6.3.3: Usar os serviços da AWS para avaliar a conformidade da arquitetura com relação às práticas recomendadas de segurança da AWS (por exemplo, a ferramenta AWS Well-Architected Framework).

Apêndice A

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

Serviços e recursos da AWS dentro do 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:

Analytics:

- Amazon Athena
- Amazon OpenSearch Service

Integração de aplicações:

- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

Computação:

- Amazon API Gateway
- Amazon EC2 (incluindo EC2 Image Builder, EC2 Instance Connect)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EMR
- AWS Lambda
- Amazon Data Lifecycle Manager

Ferramentas do desenvolvedor

- AWS Fault Injection Service

Internet das Coisas

- AWS IoT Core

Machine learning:

- Amazon Bedrock
- Amazon CodeGuru Security
- Amazon Q Business
- Amazon Q Developer
- Amazon SageMaker IA

Gerenciamento e governança:

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- Hub de Resiliência da AWS
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor
- Notificações de Usuários da AWS
- AWS Well-Architected Tool

Redes e entrega de conteúdo:

- Controlador de Recuperação de Aplicações da Amazon
- Amazon VPC
    - Network Access Analyzer
    - ACLs de rede
    - Grupos de segurança
    - Endpoints da VPC
    - AWS Site-to-Site VPN
    - Logs de fluxo
    - Endpoints da VPC
    - Acesso Verificado pela AWS
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53 (incluindo o Route 53 Resolver DNS Firewall)
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- Network Access Analyzer
- AWS Transit Gateway

Segurança, identidade e conformidade:

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Automated Forensics Orchestrator para Amazon EC2
- Amazon GuardDuty
- Centro de Identidade do AWS IAM
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall

- AWS Private Certificate Authority
- AWS Secrets Manager
- AWS Security Hub
- Amazon Security Lake
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS Shield Avançado
- AWS WAF

Armazenamento e gerenciamento de dados:

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon Elastic File System (Amazon EFS) (incluindo políticas de ciclo de vida do EFS)
- Amazon FSx para Lustre

Serviços e recursos 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 aos cargos desejados para o exame foram excluídas dessa lista:

Integração de aplicações:

- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)

Segurança, identidade e conformidade:

- AWS Payment Cryptography

Apêndice B: Comparação entre SCS-C02 e SCS- C03

Comparação lado a lado

A tabela a seguir mostra os domínios e a porcentagem de perguntas pontuadas em cada domínio do exame SCS-C02 (em uso até 1.º de dezembro de 2025) e do exame SCS-C03 (em uso a partir de 2 de dezembro de 2025).

Domínio do SCS-C02	Domínio do SCS-C03
Domínio 1: Detecção de ameaças e resposta a incidentes (14%)	Domínio do conteúdo 1: Detecção (16% do conteúdo pontuado)
Domínio 2: Registro e monitoramento de segurança (18%)	Domínio do conteúdo 2: Resposta a incidentes (14%)
Domínio 3: Segurança de infraestrutura (20%)	Domínio do conteúdo 3: Segurança de infraestrutura (18%)
Domínio 4: Gerenciamento de identidade e acesso (16%)	Domínio do conteúdo 4: Gerenciamento de identidade e acesso (20%)
Domínio 5: Proteção de dados (18%)	Domínio do conteúdo 5: Proteção de dados (18%)
Domínio 6: Gerenciamento e governança de segurança (14%)	Domínio do conteúdo 6: Governança e fundamentos de segurança (14%)

Conteúdo adicionado ao SCS-C03

Na Tarefa 2.2.3, o seguinte conteúdo foi adicionado:

- 2.2.3 Validar as descobertas dos serviços de segurança da AWS para avaliar o escopo e o impacto de um evento.

Na Tarefa 3.1.4, o seguinte conteúdo foi adicionado:

- 3.1.4 Configurar integrações com serviços de borda da AWS e serviços de terceiros (por exemplo, ingerir dados no formato Open Cybersecurity Schema Framework [OCSF], usando regras WAF de terceiros).

Na Tarefa 3.2.7, o seguinte conteúdo foi adicionado:

- 3.2.7 Implementar proteções e barreiras de proteção para aplicações de IA generativa (por exemplo, aplicar as proteções do Top 10 de IA generativa do OWASP para aplicações de LLM).

Na Tarefa 5.1.3, o seguinte conteúdo foi adicionado:

- 5.1.3 Projetar e configurar a criptografia entre recursos em trânsito (por exemplo, configurações de criptografia entre nós para Amazon EMR, Amazon Elastic Kubernetes Service [Amazon EKS], SageMaker IA, criptografia Nitro).

Na Tarefa 5.3.3, o seguinte conteúdo foi adicionado:

- 5.3.3 Descrever as diferenças entre o material de chave importado e o material de chave gerado pela AWS.

Na Tarefa 5.3.4, o seguinte conteúdo foi adicionado:

- 5.3.4 Mascarar dados sensíveis (por exemplo, políticas de proteção de dados do CloudWatch Logs, proteção de dados de mensagens do Amazon Simple Notification Service [Amazon SNS]).

Na Tarefa 5.3.5, o seguinte conteúdo foi adicionado:

- 5.3.5 Criar e gerenciar chaves de criptografia e certificados em uma única Região AWS ou em várias regiões (por exemplo, chaves do AWS KMS gerenciadas pelo cliente do AWS KMS, AWS Private Certificate Authority).

Conteúdo excluído do SCS-C03

Na Tarefa 6.4, o seguinte conteúdo foi removido:

- Identificar as falhas de segurança por meio de avaliações de arquitetura e análise de custos.

Na Tarefa 1.1, o seguinte conteúdo foi removido:

- Formato de busca de segurança da AWS (ASFF)

Na Tarefa 1.3, o seguinte conteúdo foi removido:

- Guia de resposta a incidentes de segurança da AWS

Na Tarefa 2.5, o seguinte conteúdo foi removido:

- Formato e componentes do log (por exemplo, logs do CloudTrail)

Na Tarefa 3.3, o seguinte conteúdo foi removido:

- Segurança baseada em host (por exemplo, firewalls, proteção)
- Ativar mecanismos de segurança baseados em host (por exemplo, firewalls baseados em host)

Na Tarefa 3.4, o seguinte conteúdo foi removido:

- 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)
- Identificar, interpretar e priorizar problemas na conectividade de rede (por exemplo, usando o Amazon Inspector Network Reachability)

Na Tarefa 4.2, o seguinte conteúdo foi removido:

- Componentes e impacto de uma política (por exemplo, principal, ação, recurso, condição)

Na Tarefa 5.1, o seguinte conteúdo foi removido:

- Conceitos de TLS
- Projetar redes entre regiões usando VIFs privadas e VIFs públicas

Na Tarefa 5.2, o seguinte conteúdo foi removido:

- Configurar hospedagem de sites estáticos do S3.

Recategorizações de conteúdo do SCS-C03

Estas foram as principais reorganizações de conteúdo que ocorreram na transição do SCS-C02 para o SCS-C03:

Os domínios 1 e 2 do SCS-C02 foram reestruturados:

- “Detecção de ameaças e resposta a incidentes” e “Registro em log e monitoramento de segurança” agora são:
    - Domínio 1: Detecção
    - Domínio 2: Resposta a incidentes

O domínio 6 foi renomeado no SCS-C03:

- De “Gerenciamento e governança de segurança” para “Governança e fundamentos de segurança”

A seguinte declaração de tarefa foi recategorizada:

A declaração da tarefa 1.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.
- 1.2 Projetar e implementar o registro em log.
- 2.1 Projetar e testar um plano de resposta a incidentes.
- 2.2 Responder a eventos de segurança.

A declaração da tarefa 1.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.
- 1.2 Projetar e implementar o registro em log.

A declaração da Tarefa 1.3 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 2.1 Projetar e testar um plano de resposta a incidentes.
- 2.2 Responder a eventos de segurança.

A declaração da tarefa 2.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.

A declaração da tarefa 2.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.

- 1.2 Projetar e implementar o registro em log.
- 1.3 Solucionar problemas de registro em log, alertas e monitoramento da segurança.

A declaração da tarefa 2.3 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.

A declaração da tarefa 2.4 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.
- 1.3 Solucionar problemas de registro em log, alertas e monitoramento da segurança.

A declaração da tarefa 2.5 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.

A declaração da tarefa 3.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.
- 3.1 Projetar, implementar e solucionar problemas de controles de segurança para serviços de borda da rede.

A declaração da tarefa 3.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.
- 3.3 Projetar e solucionar problemas de controles de segurança de rede.
- 5.1 Projetar e implementar controles para dados em trânsito.
- 6.2 Implementar uma estratégia de implantação segura e consistente para recursos de nuvem.

A declaração da tarefa 3.3 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 3.2 Projetar, implementar e solucionar problemas de controles de segurança para workloads de computação.
- 5.3 Projetar e implementar controles para proteger dados confidenciais, segredos e materiais de chaves criptográficas.

A declaração da tarefa 3.4 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.2 Projetar e implementar o registro em log.
- 3.3 Projetar e solucionar problemas de controles de segurança de rede.

A declaração da tarefa 4.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 4.1 Projetar, implementar e solucionar problemas de estratégias de autenticação

A declaração da tarefa 4.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 4.2 Projetar, implementar e solucionar problemas de estratégias de autorização

A declaração da tarefa 5.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 3.2 Projetar, implementar e solucionar problemas de controles de segurança para workloads de computação.
- 3.3 Projetar e solucionar problemas de controles de segurança de rede.
- 5.1 Projetar e implementar controles para dados em trânsito.

A declaração da tarefa 5.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 4.2 Projetar, implementar e solucionar problemas de estratégias de autorização
- 5.2 Projetar e implementar controles para dados em repouso.

A declaração da tarefa 5.3 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 5.2 Projetar e implementar controles para dados em repouso.

A declaração da tarefa 5.4 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 5.2 Projetar e implementar controles para dados em repouso.
- 5.3 Projetar e implementar controles para proteger dados confidenciais, segredos e materiais de chaves criptográficas.

A declaração da tarefa 6.1 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 4.2 Projetar, implementar e solucionar problemas de estratégias de autorização
- 6.1 Desenvolver uma estratégia para implantar e gerenciar de maneira centralizada as contas da AWS.

A declaração da tarefa 6.2 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 6.2 Implementar uma estratégia de implantação segura e consistente para recursos de nuvem.

A declaração da tarefa 6.3 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.

- 5.2 Projetar e implementar controles para dados em repouso.
- 6.3 Avaliar a conformidade dos recursos da AWS.

A declaração da tarefa 6.4 do SCS-C02 é mapeada para as seguintes tarefas no SCS-C03:

- 2.1 Projetar e testar um plano de resposta a incidentes.
- 1.1 Projetar e implementar monitoramento e alertas para uma organização ou conta da AWS.
- 6.3 Avaliar a conformidade dos recursos da AWS.

Pesquisa

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