考试指南 (SCS-C03)

AWS Certified Security - Specialty

AWS Certified Security - Specialty: 考试指南 (SCS-C03)

Table of Contents

AWS Certified Security - Specialty (SCS-C03)

AWS Certified Security - Specialty 考试面向负责确保云解决方案安全的个人。本考试旨在检验考生在有效展示有关保护 AWS 产品和服务的知识方面的能力。

主题

简介

AWS Certified Security - Specialty 考试面向负责确保云解决方案安全的个人。本考试旨在检验考生在有效展示有关保护 AWS 产品和服务的知识方面的能力。

本考试还考查考生完成以下任务的能力：

- 应用专业数据分类方法及 AWS 数据保护机制。

- 实施数据加密方法及 AWS 加密机制。
- 实施 AWS 机制来遵循互联网安全协议。
- 使用 AWS 安全服务和功能，确保生产环境的安全。
- 权衡成本、安全性和部署复杂性等考量因素，制订决策，满足一系列应用要求。
- 了解安全操作以及风险。

目标考生说明

目标考生应具有相当于 3-5 年的保障云解决方案安全的经验。

建议掌握的 AWS 知识

目标考生应具备以下 AWS 知识：

- AWS 责任共担模式及其应用
- 大规模管理身份
- 多账户监管
- 管理软件供应链风险
- 安全事件预防和响应策略
- 云中的漏洞管理
- 为第 3 层至第 7 层制定大规模的防火墙规则
- 事件根本原因分析
- 应对审计的经验
- 日志记录和监控策略
- 静态和传输中的数据加密方法
- 灾难恢复控制，包括备份策略

超出目标考生考试范围的工作任务

下表所列为目标考生无需具备执行能力的各项工作任务。此列表并非详尽无遗。以下任务超出考试范围：

- 设计加密算法

- 在数据包层面分析流量
- 设计整体云部署架构
- 管理终端用户的计算资源
- 训练机器学习模型

考试内容

答案类型

考试包含以下一种或多种题型：

- 单选题： 具有一个正确答案和三个错误答案（干扰项）
- 多选题： 在五个或更多答案选项中具有两个或更多正确答案
- 排序题： 列出完成指定任务可能需要的 3 至 5 个答案。您必须选择正确的答案并按正确的顺序排列答案，才能得分。
- 配对题： 采用一列提示和一列答案的形式，提示列有 3 至 7 条提示。您必须将所有答案与提示正确匹配才能得分。

未回答的试题计为回答不正确。猜答案不会扣分。本考试包括 50 道试题，这些试题将影响您的分数。

不计分内容

本考试包括 15 道不计分试题，这些试题不影响您的分数。AWS 收集这些不计分试题的答题情况进行评估，以便将来将这些试题作为计分试题。在考试中不会标明这些不计分试题。

考试结果

AWS Certified Security - Specialty (SCS-C03) 考试成绩分为及格和不及格两种。本考试按照 AWS 专业人员根据认证行业最佳实践和准则制定的最低标准进行评分。

您的考试结果换算分数为 100-1000 分。最低及格分数为 750 分。您的分数表明您的总体考试答题情况以及是否通过考试。标准分模型有助于将难易程度可能略有不同的多种考试形式中的分数进行公平处理。

您的成绩单可能包含一个分类表，其中列出您在每个部分的考试成绩。本考试采用补偿评分模型，这意味着您无需在每个部分都达到及格分数。您只需通过整体考试即可。

考试的每个部分具有特定的权重，因此，某些部分的试题比其他部分多。分类表包含常规信息，用于突出显示您的强项和弱项。在解读各个部分的反馈时，请务必小心谨慎。

内容大纲

本考试指南包括考试的权重、内容领域和任务说明，并未列出考试的全部内容。

考试中考查的内容领域和相应的权重如下：

服务参考资料

以下各节提供与本认证考试相关的 AWS 服务、技术和概念的详细信息：

- 考试范围内的 AWS 服务
- 考试范围外的 AWS 服务
- 技术和概念

内容领域 1： 检测

任务

任务 1.1： 为 AWS 账户或企业设计并实施监控和警报解决方案。

具备以下技能：

- 技能 1.1.1： 分析工作负载来确定监控需求。
- 技能 1.1.2： 设计和实施工作负载监控策略（例如：配置资源运行状况检查）。
- 技能 1.1.3： 汇总安全和监控事件。
- 技能 1.1.4： 创建指标、警报和控制面板，用于检测异常数据和事件（例如：Amazon GuardDuty、Amazon Security Lake、AWS Security Hub、Amazon Macie）。
- 技能 1.1.5： 创建和管理自动化功能，用于执行定期评估和调查（例如：部署 AWS Config 合规包、Security Hub、AWS Systems Manager 状态管理器）。

任务 1.2： 设计和实施日志记录解决方案

具备以下技能：

- 技能 1.2.1： 根据要求，确定日志摄取和存储的来源。
- 技能 1.2.2： 为 AWS 服务和应用程序配置日志记录（例如：为企业配置 AWS CloudTrail 跟踪记录、创建专用的 Amazon CloudWatch 日志记录账户、配置 Amazon CloudWatch Logs 代理）。
- 技能 1.2.3： 实施日志存储和日志数据湖（例如：Security Lake），并集成第三方安全工具。
- 技能 1.2.4： 使用 AWS 服务分析日志（例如：CloudWatch Logs Insights、Amazon Athena、Security Hub 发现）。
- 技能 1.2.5： 使用 AWS 服务标准化、解析和关联日志（例如：Amazon OpenSearch Service、AWS Lambda、Amazon Managed Grafana）。
- 技能 1.2.6： 根据网络设计、威胁和攻击情况，确定并配置合适的日志源（例如：VPC 流日志、Transit Gateway 流日志、Amazon Route 53 Resolver 日志）。

任务 1.3： 排查安全监控、日志记录和警报解决方案

具备以下技能：

- 技能 1.3.1： 分析资源的功能、权限和配置（例如：Lambda 函数日志记录、Amazon API Gateway 日志记录、运行状况检查、Amazon CloudFront 日志记录）。
- 技能 1.3.2： 修复资源配置错误（例如：排查 CloudWatch 代理的配置问题、排查缺失的日志）。

内容领域 2： 事件响应

任务

任务 2.1： 设计和测试事件响应计划。

具备以下技能：

- 技能 2.1.1： 设计并实施响应计划和运行手册，来应对安全事件（例如：Systems Manager OpsCenter、Amazon SageMaker AI 笔记本）。
- 技能 2.1.2： 利用 AWS 服务特性和功能配置服务，来为应对各种事件做好准备（例如：预置访问权限、部署安全工具、尽可能缩小影响范围、配置 AWS Shield Advanced 保护措施）。
- 技能 2.1.3： 推荐用于测试和验证事件响应计划有效性的程序（例如：AWS 故障注入服务、AWS 韧性监测中心）。
- 技能 2.1.4： 使用 AWS 服务自动修复事件（例如：Systems Manager、适用于 Amazon EC2 的自动化取证编排工具、AWS Step Functions、Amazon 应用程序恢复控制器、Lambda 函数）。

任务 2.2： 响应安全事件

具备以下技能：

- 技能 2.2.1： 捕获相关的系统和应用程序日志，并将其存储为取证文档。
- 技能 2.2.2： 跨应用程序和 AWS 服务，搜索并关联安全事件的日志。
- 技能 2.2.3： 验证 AWS 安全服务的发现，评估事件的范围和影响。
- 技能 2.2.4： 对受影响的资源采取行动，遏制和根除威胁并恢复资源（例如：实施网络控制措施、恢复备份）。
- 技能 2.2.5： 描述开展根本原因分析的方法（例如：Amazon Detective）。

内容领域 3： 基础设施安全性

任务

任务 3.1： 针对网络边缘服务，设计、实施安全控制措施，以及进行故障排除

具备以下技能：

- 技能 3.1.1： 根据预计的威胁和攻击，定义和选择边缘安全策略。
- 技能 3.1.2： 实施适当的网络边缘保护措施（例如：CloudFront 标头、AWS WAF、AWS IoT 策略、防御 OWASP 十大威胁、Amazon S3 跨源资源共享 [CORS]、Shield Advanced）。
- 技能 3.1.3： 根据要求（例如：地理位置、定位、速率限制、客户端指纹识别），设计和实施 AWS 边缘控制措施和规则。
- 技能 3.1.4： 配置与 AWS 边缘服务和第三方服务的集成（例如：以 Open Cybersecurity Schema Framework [OCSF] 格式摄取数据，使用第三方 WAF 规则等）。

任务 3.2： 针对计算工作负载，设计、实施安全控制措施，以及进行故障排除

具备以下技能：

- 技能 3.2.1： 设计和实施强化的 Amazon EC2 AMI 和容器映像，用于保护计算工作负载并嵌入安全控制措施（例如：Systems Manager、EC2 Image Builder）。
- 技能 3.2.2： 正确地应用实例配置文件、服务角色和执行角色，用于授权计算工作负载。
- 技能 3.2.3： 扫描计算资源中是否存在已知漏洞（例如：使用 Amazon Inspector 扫描容器映像和 Lambda 函数，使用 GuardDuty 监控计算运行时）。
- 技能 3.2.4： 实施自动更新流程并集成持续验证方法（例如：Systems Manager 补丁管理器、Amazon Inspector），来跨计算资源部署补丁，确保环境安全且合规。
- 技能 3.2.5： 配置对计算资源进行安全的管理访问（例如：Systems Manager Session Manager、EC2 Instance Connect）。
- 技能 3.2.6： 配置安全工具，发现和修复管道中的漏洞（例如：Amazon Q Developer、Amazon CodeGuru 安全防御工具）。
- 技能 3.2.7： 为生成式人工智能应用程序实施保护和防护机制（例如：根据 OWASP 生成式人工智能十大安全风险，保护大型语言模型应用程序）。

任务 3.3： 设计网络安全控制措施，以及进行故障排除

具备以下技能：

- 技能 3.3.1： 设计相应的网络控制措施，根据需要允许或阻止网络流量，以及进行故障排除（例如：安全组、网络 ACL、AWS Network Firewall）。
- 技能 3.3.2： 设计混合环境和多云网络之间的安全连接（例如：AWS Site-to-Site VPN、AWS Direct Connect、MAC Security [MACsec]）。
- 技能 3.3.3： 针对混合环境与 AWS 之间的通信，确定并配置安全工作负载要求（例如：使用 AWS Verified Access）。
- 技能 3.3.4： 根据安全要求设计网络分段（例如：北/南流量和东/西流量保护、隔离子网）。
- 技能 3.3.5： 识别不必要的网络访问（例如：AWS Verified Access、Network Access Analyzer、Amazon Inspector Network Reachability 发现）。

内容领域 4： 身份和访问管理

任务

任务 4.1： 设计和实施身份验证策略，以及进行故障排除

具备以下技能：

- 技能 4.1.1： 设计并建立用于人员、应用程序和系统身份验证的身份解决方案（例如：AWS IAM Identity Center、Amazon Cognito、多重身份验证 [MFA]、身份提供商 [IdP] 集成）。
- 技能 4.1.2： 配置颁发临时凭证的机制（例如：AWS STS、Amazon S3 预签名 URL）。
- 技能 4.1.3： 排查身份验证问题（例如：CloudTrail、Amazon Cognito、IAM Identity Center 权限集、AWS Directory Service）。

任务 4.2： 设计和实施授权策略，以及进行故障排除

具备以下技能：

- 技能 4.2.1： 设计并评估面向人员、应用程序和系统访问的授权控制措施（例如：Amazon Verified Permissions、IAM 路径、IAM Roles Anywhere、跨账户访问的资源策略、IAM 角色信任策略）。
- 技能 4.2.2： 设计基于属性的访问控制 (ABAC) 策略和基于角色的访问控制 (RBAC) 策略（例如：配置基于标签或属性的资源访问）。
- 技能 4.2.3： 遵循最低权限原则来设计、解释和实施 IAM 策略（例如：权限边界、会话策略）。
- 技能 4.2.4： 分析授权故障来确定原因或影响（例如：IAM 策略模拟器、IAM 访问权限分析器）。
- 技能 4.2.5： 调查并更正向资源、服务或实体意外授予的权限、授权或特权（例如：IAM 访问权限分析器）。

内容领域 5： 数据保护

任务

- 任务 5.1： 为传输中的数据设计和实施控制措施
- 任务 5.2： 针对静态数据设计和实施控制措施
- 任务 5.3： 设计和实施控制措施，用于保护机密数据、凭证、密钥和加密密钥材料。

任务 5.1： 为传输中的数据设计和实施控制措施

具备以下技能：

- 技能 5.1.1： 设计并配置在连接资源时要求进行加密的机制（例如：配置弹性负载均衡 [ELB] 安全策略，强制执行 TLS 配置）。
- 技能 5.1.2： 设计并配置用于安全私密地访问资源的机制（例如：AWS PrivateLink、VPC 端点、AWS Client VPN、AWS Verified Access）。
- 技能 5.1.3： 设计并配置资源间的传输中加密（例如：针对 Amazon EMR、Amazon EKS、SageMaker AI 的节点间加密配置，Nitro 加密）。

任务 5.2： 针对静态数据设计和实施控制措施

具备以下技能：

- 技能 5.2.1： 根据特定要求，设计、实施和配置静态数据加密（例如：选择 AWS CloudHSM 或 AWS KMS 等合适的加密密钥服务，或者选择客户端加密或服务器端加密等合适的加密类型）。

- 技能 5.2.2： 设计并配置保护数据完整性的机制（例如：S3 对象锁定、S3 Glacier 文件库锁定、版本控制、数字代码签名、文件验证）。
- 技能 5.2.3： 为数据设计自动生命周期管理和保留解决方案（例如：S3 生命周期策略、S3 对象锁定、Amazon EFS 生命周期策略、适用于 Lustre 的 Amazon FSx 备份策略）。
- 技能 5.2.4： 设计并配置安全的数据复制和备份解决方案（例如：Amazon Data Lifecycle Manager、AWS Backup、勒索软件防护、AWS DataSync）。

任务 5.3： 设计和实施控制措施，用于保护机密数据、凭证、密钥和加密密钥材料。

具备以下技能：

- 技能 5.3.1： 设计凭证及密钥的管理和轮换机制（例如：AWS Secrets Manager）。
- 技能 5.3.2： 管理和使用导入的密钥材料（例如：管理和轮换导入的密钥材料，管理和配置外部密钥存储）。
- 技能 5.3.3： 说明导入的密钥材料与 AWS 生成的密钥材料之间的区别。
- 技能 5.3.4： 掩蔽敏感数据（例如：CloudWatch Logs 数据保护策略、Amazon SNS 消息数据保护）。
- 技能 5.3.5： 在单个或多个 AWS 区域中，创建并管理加密密钥和证书（例如：AWS KMS 客户自主管理型 AWS KMS 密钥、AWS 私有证书颁发机构）。

内容领域 6： 安全基础与监管

任务

任务 6.1： 制定策略来集中部署和管理 AWS 账户

具备以下技能：

- 技能 6.1.1： 使用 AWS Organizations 部署和配置企业。

- 技能 6.1.2： 在新环境和现有环境中实施并管理 AWS Control Tower，部署可选和自定义的控制措施。
- 技能 6.1.3： 实施企业策略来管理权限（例如：SCP、RCP、AI 服务选择退出策略、声明性策略）。
- 技能 6.1.4： 集中管理安全服务（例如：委派管理员帐户）。
- 技能 6.1.5： 管理 AWS 账户根用户凭证（例如：集中成员账户的根访问权限、管理 MFA、设计破译程序）。

任务 6.2： 为云资源实施安全且一致的部署策略

具备以下技能：

- 技能 6.2.1： 使用基础设施即代码 (IaC)，以一致的方式，安全地跨账户部署云资源（例如：CloudFormation 堆栈集、第三方 IaC 工具、CloudFormation Guard、cfn-lint）。
- 技能 6.2.2： 使用标签将 AWS 资源分组，方便进行管理（例如：按部门、成本中心、环境分组）。
- 技能 6.2.3： 从中心来源部署并执行策略和配置（例如：AWS Firewall Manager）。
- 技能 6.2.4： 在 AWS 账户之间安全地共享资源（例如：AWS Service Catalog、AWS Resource Access Manager [AWS RAM]）。

任务 6.3： 评估 AWS 资源的合规性

具备以下技能：

- 技能 6.3.1： 创建或启用规则，用于检测和修复不合规的 AWS 资源并发送通知（例如：使用 AWS Config 汇总警报和修复不合规资源，Security Hub）。
- 技能 6.3.2： 使用 AWS 审计服务来收集和整理证据（例如：AWS Audit Manager、AWS Artifact）。
- 技能 6.3.3： 使用 AWS 服务，根据 AWS 安全最佳实践评估架构的合规性（例如：AWS Well-Architected Framework 工具）。

考试范围内的 AWS 服务

注意： 安全性将影响所有 AWS 服务。许多服务并未列入此列表，因为该服务整体属于范围外，而服务的安全方面则在考核范围内。例如，本考试的考生不需要了解为 S3 存储桶配置复制的步骤。但是，考生可能会被问及有关配置 S3 存储桶策略的问题。

下表列出了考试范围内的 AWS 服务和功能。此列表并非详尽无遗，并且可能随时会更改。AWS 各项产品和服务按其主要功能进行分类：

主题

分析

- Amazon Athena
- Amazon OpenSearch Service

应用程序集成

- Amazon SNS
- AWS Step Functions

计算

- Amazon API Gateway
- Amazon EC2（包括 EC2 Image Builder、EC2 Instance Connect）
- Amazon EKS
- Amazon EMR
- AWS Lambda

- Amazon Data Lifecycle Manager

开发工具

- AWS 故障注入服务

物联网

- AWS IoT Core

机器学习

- Amazon Bedrock
- Amazon CodeGuru 安全防御工具
- Amazon Q 企业版
- Amazon Q Developer
- Amazon SageMaker AI

管理和监管

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- AWS 韧性监测中心
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog

- AWS Systems Manager
- AWS Trusted Advisor
- AWS 用户通知服务
- AWS Well-Architected Tool

联网和内容分发

- Amazon 应用程序恢复控制器
- Amazon VPC
  - Network Access Analyzer
  - 网络 ACL
  - 安全组
  - VPC 端点
  - AWS Site-to-Site VPN
  - 流日志
  - VPC 端点
  - AWS Verified Access
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53（包括 Route 53 Resolver DNS 防火墙）
- AWS Direct Connect
- 弹性负载均衡 (ELB)
- Network Access Analyzer
- AWS Transit Gateway

安全性、身份与合规性

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)

- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- 适用于 Amazon EC2 的自动化取证编排工具
- Amazon GuardDuty
- IAM
- AWS IAM Identity Center
- Amazon Inspector
- AWS KMS
- Amazon Macie
- AWS Network Firewall
- AWS Private Certificate Authority
- AWS Secrets Manager
- AWS Security Hub
- Amazon Security Lake
- AWS Shield
- AWS Shield Advanced
- AWS STS
- AWS WAF

存储和数据管理

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon EFS（包括 EFS 生命周期策略）
- 适用于 Lustre 的 Amazon FSx

考试范围外的 AWS 服务

下表列出了考试范围外的 AWS 服务和功能。此列表并非详尽无遗，并且可能随时会更改。与考试目标职位完全无关的 AWS产品和服务的内容，均未包含在本表中：

主题

应用程序集成

- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)

安全性、身份与合规性

- AWS Payment Cryptography

技术和概念

以下列表包含考试中可能出现的技术和概念。此列表并非详尽无遗，并且可能随时会更改。表中各项的顺序与位置，并不代表考试中的相对权重或重要性：

- AWS CLI
- AWS SDK
- AWS 管理控制台
- 安全远程访问
- 证书管理
- 基础设施即代码 (IaC)

附录： SCS-C02 与 SCS-C03 的比较

并排比较

下表显示了在 SCS-C02 考试（在 2025 年 12 月 1 日之前使用）和 SCS-C03 考试（于 2025 年 12 月 2 日起使用）中，所涉及的领域和每个领域中计分问题的百分比。

SCS-C02 领域	SCS-C03 领域
领域 1： 威胁检测和事件响应（占计分内容的 14%）	内容领域 1： 检测（占计分内容的 16%）
领域 2： 安全日志记录和监控（占计分内容的 18%）	内容领域 2： 事件响应（占计分内容的 14%）
领域 3： 基础设施安全性（占计分内容的 20%）	内容领域 3： 基础设施安全性（占计分内容的 18%）
领域 4： 身份和访问管理（占计分内容的 16%）	内容领域 4： 身份和访问管理（占计分内容的 20%）
领域 5： 数据保护（占计分内容的 18%）	内容领域 5： 数据保护（占计分内容的 18%）
领域 6： 管理和安全监管（占计分内容的 14%）	内容领域 6： 安全基础与监管（占计分内容的 14%）

SCS-C03 的内容增补

任务 2.2.3 中添加了以下内容：

- 2.2.3 验证 AWS 安全服务的发现，评估事件的范围和影响。

任务 3.1.4 中添加了以下内容：

- 3.1.4 配置与 AWS 边缘服务和第三方服务的集成（例如：以 Open Cybersecurity Schema Framework [OCSF] 格式摄取数据，使用第三方 WAF 规则等）。

任务 3.2.7 中添加了以下内容：

- 3.2.7 为生成式人工智能应用程序实施保护和防护机制（例如：根据 OWASP 生成式人工智能十大安全风险，保护大型语言模型应用程序）。

任务 5.1.3 中添加了以下内容：

- 5.1.3 设计并配置资源间的传输中加密（例如：针对 Amazon EMR、Amazon Elastic Kubernetes Service [Amazon EKS]、SageMaker AI 的节点间加密，Nitro 加密）。

任务 5.3.3 中添加了以下内容：

- 5.3.3 说明导入的密钥材料与 AWS 生成的密钥材料之间的区别。

任务 5.3.4 中添加了以下内容：

- 5.3.4 掩蔽敏感数据（例如：CloudWatch Logs 数据保护策略、Amazon Simple Notification Service [Amazon SNS] 消息数据保护）。

任务 5.3.5 中添加了以下内容：

- 5.3.5 在单个或多个 AWS 区域中，创建并管理加密密钥和证书（例如：AWS KMS 客户自主管理型 AWS KMS 密钥、AWS 私有证书颁发机构）。

SCS-C03 的内容删减

任务 6.4 中删除了以下内容：

- 通过架构审核和成本分析找出安全漏洞。

任务 1.1 中删除了以下内容：

- AWS Security Finding Format (ASFF)

任务 1.3 中删除了以下内容：

- AWS 安全事件响应指南

任务 2.5 中删除了以下内容：

- 日志格式和组件（例如：CloudTrail 日志）

任务 3.3 中删除了以下内容：

- 基于主机的安全性（例如防火墙、强化）
- 激活基于主机的安全机制（例如基于主机的防火墙）

任务 3.4 中删除了以下内容：

- 如何分析可访问性（例如：使用 VPC Reachability Analyzer 和 Amazon Inspector）
- 基本 TCP/IP 联网概念（例如：UDP 与 TCP 的比较、端口、开放系统互连 [OSI] 模型、网络操作系统实用程序）
- 找出和解释网络连接中的问题并确定其优先级（例如：使用 Amazon Inspector Network Reachability）

任务 4.2 中删除了以下内容：

- 策略的组成部分和影响（例如主体、操作、资源、条件）

任务 5.1 中删除了以下内容：

- TLS 概念
- 使用私有 VIF 和公有 VIF 设计跨区域联网

任务 5.2 中删除了以下内容：

- 配置 S3 静态网站托管。

SCS-C03 内容的重新分类

在从 SCS-C02 过渡到 SCS-C03 的过程中，以下主要内容进行了重新排列：

SCS-C03 领域 1 和 2 的结构进行了重新设计：

- “威胁检测和事件响应” 和 “安全日志记录和监控” 现在分别为：

- 领域 1： 检测
- 领域 2： 事件响应

SCS-C03 的领域 6 已重命名：

- 从 “管理和安全监管” 改为 “安全基础与监管”

以下任务说明已重新分类：

SCS-C02 任务说明 1.1 对应于 SCS-C03 中的以下任务：

- 1.1 为 AWS 账户或企业设计并实施监控和警报。
- 1.2 设计和实施日志记录。
- 2.1 设计和测试事件响应计划。
- 2.2 响应安全事件。

SCS-C02 任务说明 1.2 对应于 SCS-C03 中的以下任务：

- 1.1 为 AWS 账户或企业设计并实施监控和警报。
- 1.2 设计和实施日志记录。

SCS-C02 任务说明 1.3 对应于 SCS-C03 中的以下任务：

- 2.1 设计和测试事件响应计划。
- 2.2 响应安全事件。

SCS-C02 任务说明 2.1 对应于 SCS-C03 中的以下任务：

- 1.1 为 AWS 账户或企业设计并实施监控和警报。

SCS-C02 任务说明 2.2 对应于 SCS-C03 中的以下任务：

- 1.1 为 AWS 账户或企业设计并实施监控和警报。
- 1.2 设计和实施日志记录。
- 1.3 排查安全监控、日志记录和警报。

SCS-C02 任务说明 2.3 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。

SCS-C02 任务说明 2.4 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。
- 1.3 排查安全监控、日志记录和警报。

SCS-C02 任务说明 2.5 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。

SCS-C02 任务说明 3.1 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。
- 3.1 针对网络边缘服务，设计、实施安全控制措施，以及进行故障排除。

SCS-C02 任务说明 3.2 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。
- 3.3 设计网络安全控制措施，以及进行故障排除。
- 5.1 为传输中的数据设计和实施控制措施。
- 6.2 为云资源实施安全且一致的部署策略。

SCS-C02 任务说明 3.3 对应于 SCS-C03 中的以下任务：

- 3.2 针对计算工作负载，设计、实施安全控制措施，以及进行故障排除。
- 5.3 设计和实施控制措施，用于保护机密数据、凭证、密钥和加密密钥材料。

SCS-C02 任务说明 3.4 对应于 SCS-C03 中的以下任务：

- 1.2 设计和实施日志记录。
- 3.3 设计网络安全控制措施，以及进行故障排除。

SCS-C02 任务说明 4.1 对应于 SCS-C03 中的以下任务：

- 4.1 设计和实施身份验证策略，以及进行故障排除。

SCS-C02 任务说明 4.2 对应于 SCS-C03 中的以下任务：

- 4.2 设计和实施授权策略，以及进行故障排除。

SCS-C02 任务说明 5.1 对应于 SCS-C03 中的以下任务：

- 3.2 针对计算工作负载，设计、实施安全控制措施，以及进行故障排除。
- 3.3 设计网络安全控制措施，以及进行故障排除。
- 5.1 为传输中的数据设计和实施控制措施。

SCS-C02 任务说明 5.2 对应于 SCS-C03 中的以下任务：

- 4.2 设计和实施授权策略，以及进行故障排除。
- 5.2 针对静态数据设计和实施控制措施。

SCS-C02 任务说明 5.3 对应于 SCS-C03 中的以下任务：

- 5.2 针对静态数据设计和实施控制措施。

SCS-C02 任务说明 5.4 对应于 SCS-C03 中的以下任务：

- 5.2 针对静态数据设计和实施控制措施。
- 5.3 设计和实施控制措施，用于保护机密数据、凭证、密钥和加密密钥材料。

SCS-C02 任务说明 6.1 对应于 SCS-C03 中的以下任务：

- 4.2 设计和实施授权策略，以及进行故障排除。
- 6.1 制定策略来集中部署和管理 AWS 账户。

SCS-C02 任务说明 6.2 对应于 SCS-C03 中的以下任务：

- 6.2 为云资源实施安全且一致的部署策略。

SCS-C02 任务说明 6.3 对应于 SCS-C03 中的以下任务：

- 1.1 为 AWS 账户或企业设计并实施监控和警报。
- 5.2 针对静态数据设计和实施控制措施。
- 6.3 评估 AWS 资源的合规性。

SCS-C02 任务说明 6.4 对应于 SCS-C03 中的以下任务：

- 2.1 设计和测试事件响应计划。
- 1.1 为 AWS 账户或企业设计并实施监控和警报。
- 6.3 评估 AWS 资源的合规性。

修订

我们会定期检查并更新 AWS 考试指南，确保认证考试所考核的技能、AWS 服务和功能与认证所针对的目标工作职责相吻合。考试指南更新将提前大约一个月发布，此后这些更新才会体现在考试中。

主题

更改记录

版本	发布日期
1.0	2026 年 3 月 26 日

调查问卷

本考试指南对您有帮助吗？ 欢迎填写调查问卷，与我们分享您的建议。