# AWS Certified Security - Specialty (SCS-C02) 考试指南

## 简介

AWS Certified Security - Specialty (SCS-C02) 考试面向担任安全角色的个人。
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。

本考试还检验考生是否符合以下要求：

- 了解专门的数据分类和 AWS 数据保护机制
- 了解数据加密方法以及用于实施这些方法的 AWS 机制
- 了解安全 Internet 协议以及用于实施这些协议的 AWS 机制
- 熟练掌握用于提供安全生产环境的 AWS 安全服务和服务功能
- 在使用 AWS 安全服务和功能方面具有 2 年或以上的生产部署经验
- 能够在成本、安全性和部署复杂性方面做出权衡决策以满足一系列应用要求
- 了解安全操作和风险

## 目标考生描述

目标考生应具有 3–5 年的安全解决方案设计和实施经验或者同等经验。此外，目标考生应至少具有 2 年保护 AWS 工作负载的实践经验。

### AWS 知识推荐

目标考生应具备以下知识：

- AWS 责任共担模式及其应用
- AWS 服务和部署云科技解决方案的一般知识
- AWS 环境和工作负载的安全控制
- 日志记录和监控策略
- 漏洞管理和安全自动化
- 将 AWS 安全服务与第三方工具集成的方法
- 灾难恢复控制，包括备份策略
- 加密和密钥管理
- 身份访问管理
- 数据留存和生命周期管理
- 如何排查安全问题

- 多账户监管和企业合规性
- 威胁检测和事件响应策略

**超出目标考生考试范围的工作任务**

下表列出了不要求目标考生能够完成的相关工作任务。列表并非详尽无遗。以下任务超出考试范围：

- 使用特定语言（例如 Python、Java）开发软件。
- 确认监管合规。
- 管理软件开发生命周期。
- 设计网络拓扑。
- 设计整体云部署架构。
- 根据数据驻留要求（例如《通用数据保护条例》[GDPR]）配置存储服务。

有关考试中可能出现的技术和概念的列表、考试范围内的 AWS 服务和功能的列表，以及超出考试范围的 AWS 服务和功能的列表，请参阅附录。

## 考试内容

**答案类型**

本考试具有两种类型的试题：

- **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 5 个或更多答案选项中具有两个或更多正确答案

选择一个或多个最准确表述或回答试题的答案。干扰项或错误答案是知识或技能不全面的考生可能会选择的答案选项。干扰项通常是与内容领域相符的看似合理的答案。

未回答的试题将计为回答错误；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**

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以进行评估，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-C02) 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订的最低标准进行评分。

您的考试成绩换算分数为 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。换算评分模型有助于在难度水平可能略有不同的多种考试形式中换算分数。

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。分类表包含一般信息，用于重点说明您的强项和弱项。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、内容领域和任务表述，并未列出考试的全部内容。不过，每个任务表述都提供有额外的背景信息，有助于您备考。

考试中考查的内容领域和相应的权重如下：

- 领域 1： 威胁检测和事件响应（占计分内容的 14%）
- 领域 2： 安全日志记录和监控（占计分内容的 18%）
- 领域 3： 基础设施安全（占计分内容的 20%）
- 领域 4： 身份和访问管理（占计分内容的 16%）
- 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%）

**领域 1： 威胁检测和事件响应**

任务表述 1.1： 设计和实施事件响应计划。

掌握以下知识：

- AWS 事件响应最佳实践
- 云事件
- 事件响应计划中的角色和职责
- AWS Security Finding Format (ASFF)

具备以下技能：

- 实施凭证失效和轮换策略以应对攻击（例如，使用 AWS Identity and Access Management [IAM] 和 AWS Secrets Manager）
- 隔离 AWS 资源
- 设计和实施操作手册和运行手册以应对安全事件
- 部署安全服务（例如 AWS Security Hub、Amazon Macie、Amazon GuardDuty、Amazon Inspector、AWS Config、Amazon Detective、AWS Identity and Access Management Access Analyzer）
- 配置与原生 AWS 服务和第三方服务的集成（例如，使用 Amazon EventBridge 和 ASFF）

任务表述 1.2： 使用 AWS 服务检测安全威胁和异常。

掌握以下知识：

- 检测威胁的 AWS 托管安全服务
- 用于联接不同服务中的数据的异常和关联技术
- 用于找出异常的可视化服务
- 用于集中处理安全结果的策略

具备以下技能：

- 评估安全服务（例如 GuardDuty、Security Hub、Macie、AWS Config、IAM Access Analyzer）的结果
- 在不同的 AWS 服务中搜索和关联安全威胁（例如，使用 Detective）
- 执行查询以验证安全事件（例如，使用 Amazon Athena）
- 创建指标筛选条件和控制面板以检测异常活动（例如，使用 Amazon CloudWatch）

任务表述 1.3： 应对受到攻击的资源和工作负载。

掌握以下知识：

- AWS 安全事件响应指南
- 资源隔离机制
- 根本原因分析技术
- 数据捕获机制
- 用于事件验证的日志分析

具备以下技能：

- 使用 AWS 服务（例如 AWS Lambda、AWS Step Functions、EventBridge、AWS Systems Manager 运行手册、Security Hub、AWS Config）自动进行修复
- 应对受到攻击的资源（例如，隔离 Amazon EC2 实例）
- 调查和分析以进行根本原因分析（例如，使用 Detective）
- 从受到攻击的资源（例如 Amazon Elastic Block Store [Amazon EBS] 卷快照、内存转储）中捕获相关的取证数据
- 在 Amazon S3 中查询日志以获取与安全事件相关的上下文信息（例如，使用 Athena）
- 保护和保留取证条目（例如，使用 S3 对象锁定、隔离的取证账户、S3 生命周期和 S3 复制）
- 为事件准备服务以及在发生事件后恢复服务

**领域 2： 安全日志记录和监控**

任务表述 2.1： 设计和实施监控和告警以处理安全事件。

掌握以下知识：

- 监控事件并提供告警的 AWS 服务（例如 CloudWatch、EventBridge）
- 自动发出告警的 AWS 服务（例如 Lambda、Amazon Simple Notification Service [Amazon SNS]、Security Hub）
- 监控指标和基准的工具（例如 GuardDuty、Systems Manager）

具备以下技能：

- 分析架构以确定安全监控的监控要求和数据源
- 分析环境和工作负载以确定监控要求
- 根据业务和安全要求设计环境监控和工作负载监控
- 设置自动化工具和脚本以执行定期审核（例如，在 Security Hub 中创建自定义见解）
- 定义生成告警的指标和阈值

任务表述 2.2： 排查安全监控和告警的问题。

掌握以下知识：

- 监控服务（例如 Security Hub）的配置
- 指示安全事件的相关数据

具备以下技能：

- 在发生未提供可见性或告警的事件后分析资源的服务功能、权限和配置
- 分析和修复未报告其统计数据的自定义应用程序的配置
- 评估日志记录和监控服务是否符合安全要求

任务表述 2.3： 设计和实施日志记录解决方案。

掌握以下知识：

- 提供日志记录功能的 AWS 服务和功能（例如 VPC 流日志、DNS 日志、AWS CloudTrail、Amazon CloudWatch Logs）
- 日志记录功能属性（例如日志级别、类型、详细程度）
- 日志目标和生命周期管理（例如留存期限）

具备以下技能：

- 为服务和应用程序配置日志记录
- 确定日志摄取的日志记录要求和来源
- 根据 AWS 最佳实践和组织要求实施日志存储和生命周期管理

任务表述 2.4： 排查日志记录解决方案的问题。

掌握以下知识：

- 提供数据源的 AWS 服务的功能和使用案例（例如日志级别、类型、详细程度、频率、及时性、不变性）
- 提供日志记录功能的 AWS 服务和功能（例如 VPC 流日志、DNS 日志、CloudTrail、CloudWatch Logs）
- 日志记录所需的访问权限

具备以下技能：

- 找出错误配置，并确定缺少日志记录所需的访问权限的修复步骤（例如，管理读/写权限、S3 存储桶权限、公有访问和完整性）
- 确定缺少日志的原因并执行修复步骤

任务表述 2.5： 设计日志分析解决方案。

掌握以下知识：

- 用于对捕获的日志进行分析的服务和工具（例如 Athena、CloudWatch Logs 筛选条件）
- AWS 服务的日志分析功能（例如 CloudWatch Logs Insights、CloudTrail Insights、Security Hub Insights）

- 日志格式和组件（例如 CloudTrail 日志）

具备以下技能：

- 找出日志中的模式以指出异常和已知威胁
- 规范化、解析和关联日志

**领域 3： 基础设施安全性**

任务表述 3.1： 为边缘服务设计和实施安全控制。

掌握以下知识：

- 边缘服务上的安全功能（例如 AWS WAF、负载均衡器、Amazon Route 53、Amazon CloudFront、AWS Shield）
- 常见攻击、威胁和漏洞（例如 Open Web Application Security Project [OWASP] Top 10、DDoS）
- 分层 Web 应用程序架构

具备以下技能：

- 为常见使用案例（例如公有网站、无服务器应用程序、移动应用程序后端）定义边缘安全策略
- 根据预期的威胁和攻击（例如 OWASP Top 10、DDoS）选择相应的边缘服务
- 根据预期的漏洞和风险（例如易受攻击的软件、应用程序、库）选择相应的保护措施
- 组合使用边缘安全服务以定义防御层（例如，将 CloudFront 与 AWS WAF 和负载均衡器一起使用）
- 根据各种条件（例如地理区域、地理位置、速率限制）在边缘应用限制
- 围绕边缘服务激活日志、指标和监控以指出攻击

任务表述 3.2： 设计和实施网络安全控制。

掌握以下知识：

- VPC 安全机制（例如安全组、网络 ACL、AWS Network Firewall）
- VPC 间连接（例如 AWS Transit Gateway、VPC 终端节点）
- 安全遥测源（例如流量镜像、VPC 流日志）
- VPN 技术、术语和用法
- 本地连接选项（例如 AWS VPN、AWS Direct Connect）

具备以下技能：

- 根据安全要求实施网络分段（例如公有子网、私有子网、敏感 VPC、本地连接）
- 设计网络控制以根据需要允许或禁止网络流量（例如，使用安全组、网络 ACL 和 Network Firewall）
- 设计网络流量以使数据远离公有互联网（例如，在 VPC 中使用 Transit Gateway、VPC 终端节点和 Lambda）
- 根据网络设计、威胁和攻击确定要监控的遥测源（例如负载均衡器日志、VPC 流日志、流量镜像）
- 确定本地部署环境和 AWS 云之间通信的冗余和安全工作负载要求（例如，使用 AWS VPN、基于 Direct Connect 的 AWS VPN 和 MACsec）
- 找出和删除不必要的网络访问权限
- 根据要求变化管理网络配置（例如，使用 AWS Firewall Manager）

任务表述 3.3： 为计算工作负载设计和实施安全控制。

掌握以下知识：

- 预置和维护 EC2 实例（例如，修补、检查、创建快照和 AMI、使用 EC2 Image Builder）
- IAM 实例角色和 IAM 服务角色
- 扫描计算工作负载中的漏洞的服务（例如 Amazon Inspector、Amazon Elastic Container Registry [Amazon ECR]）
- 基于主机的安全性（例如防火墙、强化）

具备以下技能：

- 创建强化的 EC2 AMI
- 根据需要应用实例角色和服务角色以授权计算工作负载
- 扫描 EC2 实例和容器映像以查找已知漏洞
- 在一系列 EC2 实例或容器映像中应用补丁
- 激活基于主机的安全机制（例如基于主机的防火墙）
- 分析 Amazon Inspector 结果并确定相应的缓解技术
- 将密钥和凭证安全地传递到计算工作负载

任务表述 3.4： 排查网络安全问题。

掌握以下知识：

- 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）
- 如何读取相关的日志源（例如 Route 53 日志、AWS WAF 日志、VPC 流日志）

具备以下技能：

- 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）
- 确定产生所需网络行为的解决方案
- 分析日志源以找出问题
- 捕获流量样本以分析问题（例如，使用流量镜像）

**领域 4： 身份和访问管理**

任务表述 4.1： 为 AWS 资源设计和实施身份验证并进行故障排查。

掌握以下知识：

- 创建和管理身份的方法和服务（例如联合身份、身份提供程序、AWS IAM Identity Center [AWS Single Sign-On]、Amazon Cognito）
- 长期和临时认证机制
- 如何解决身份验证问题（例如，使用 CloudTrail、IAM Access Advisor 和 IAM 策略模拟器）

具备以下技能：

- 根据要求通过身份验证系统确定身份
- 设置多重身份验证 (MFA)
- 确定何时使用 AWS Security Token Service (AWS STS) 颁发临时凭证

任务表述 4.2： 为 AWS 资源设计和实施授权并排查问题。

掌握以下知识：

- 不同的 IAM 策略（例如托管策略、内联策略、基于身份的策略、基于资源的策略、会话控制策略）
- 策略的组成部分和影响（例如委托人、操作、资源、条件）
- 如何解决授权问题（例如，使用 CloudTrail、IAM Access Advisor 和 IAM 策略模拟器）

具备以下技能：

- 构建基于属性的访问控制 (ABAC) 和基于角色的访问控制 (RBAC) 策略
- 评估给定要求和工作负载的 IAM 策略类型
- 解释 IAM 策略对环境和工作负载的影响
- 在环境中应用最低权限原则
- 实施适当的职责分离
- 分析访问或授权错误以确定原因或影响
- 调查为资源、服务或实体授予的计划外权限、授权或特权

**领域 5： 数据保护**

任务表述 5.1： 设计和实施控制措施，以便为传输中的数据提供机密性和完整性。

掌握以下知识：

- TLS 概念
- VPN 概念（例如 IPsec）
- 安全远程访问方法（例如 SSH、基于 Systems Manager Session Manager 的 RDP）
- Systems Manager Session Manager 概念
- TLS 证书如何与各种网络服务和资源（例如 CloudFront、负载均衡器）一起使用

具备以下技能：

- 设计 AWS 和本地部署网络之间的安全连接（例如，使用 Direct Connect 和 VPN 网关）
- 设计机制以要求在连接到资源时进行加密（例如 Amazon RDS、Amazon Redshift、CloudFront、Amazon S3、Amazon DynamoDB、负载均衡器、Amazon Elastic File System [Amazon EFS]、Amazon API Gateway）
- 要求使用 TLS 进行 AWS API 调用（例如，使用 Amazon S3）

- 设计机制以通过安全连接转发流量（例如，使用 Systems Manager 和 EC2 Instance Connect）
- 使用私有 VIF 和公有 VIF 设计跨区域联网

任务表述 5.2： 设计和实施控制措施，以便为静态数据提供机密性和完整性。

掌握以下知识：

- 加密技术选择（例如客户端、服务器端、对称、非对称）
- 完整性检查技术（例如哈希算法、数字签名）
- 资源策略（例如 DynamoDB、Amazon S3 和 AWS Key Management Service [AWS KMS]）
- IAM 角色和策略

具备以下技能：

- 设计资源策略以仅限授权用户进行访问（例如 S3 存储桶策略、DynamoDB 策略）
- 设计机制以禁止未经授权的公有访问（例如，S3 阻止公有访问、禁止公有快照和公用 AMI）
- 配置服务以激活静态数据加密（例如 Amazon S3、Amazon RDS、DynamoDB、Amazon Simple Queue Service [Amazon SQS]、Amazon EBS、Amazon EFS）
- 设计机制以通过禁止修改保护数据完整性（例如，使用 S3 对象锁定、KMS 密钥策略、S3 Glacier 文件库锁定和 AWS Backup 文件库锁定）
- 使用 AWS CloudHSM 为关系数据库（例如 Amazon RDS、RDS Custom、EC2 实例上的数据库）设计静态加密
- 根据业务要求选择加密技术

任务表述 5.3： 设计和实施控制措施，以便管理静态数据的生命周期。

掌握以下知识：

- 生命周期策略
- 数据留存标准

具备以下技能：

- 设计 S3 生命周期机制以按照所需的留存期限来保留数据（例如 S3 对象锁定、S3 Glacier 文件库锁定、S3 生命周期策略）

- 为 AWS 服务和资源（例如 Amazon S3、EBS 卷快照、RDS 卷快照、AMI、容器映像、CloudWatch 日志组、Amazon Data Lifecycle Manager）设计自动生命周期管理
- 为不同 AWS 服务的 AWS Backup 设置计划和留存期限

任务表述 5.4： 设计和实施控制以保护凭证、密钥和加密密钥材料。

掌握以下知识：

- Secrets Manager
- Systems Manager Parameter Store
- 使用和管理对称密钥和非对称密钥（例如 AWS KMS）

具备以下技能：

- 为工作负载设计密钥管理和轮换（例如数据库访问凭证、API 密钥、IAM 访问密钥、AWS KMS 客户托管密钥）
- 设计 KMS 密钥策略以仅限授权用户使用密钥
- 建立机制以导入和删除客户提供的密钥材料

**领域 6： 管理和安全监管**

任务表述 6.1： 制定策略以集中部署和管理 AWS 账户。

掌握以下知识：

- 多账户策略
- 允许委派的管理的托管服务
- 策略定义的防护机制
- 根账户最佳实践
- 跨账户角色

具备以下技能：

- 部署和配置 AWS Organizations
- 确定何时以及如何部署 AWS Control Tower（例如，必须停用哪些服务才能成功进行部署）
- 实施 SCP 以作为执行策略的技术解决方案（例如，限制使用根账户，在 AWS Control Tower 中实施控制措施）
- 集中管理安全服务和汇总结果（例如，使用委派的管理和 AWS Config 聚合器）
- 保护 AWS 账户根用户凭证

任务表述 6.2： 为云资源实施安全且一致的部署策略。

掌握以下知识：

- 使用基础设施即代码 (IaC) 的部署最佳实践（例如 AWS CloudFormation 模板强化和偏差检测）
- 标记最佳实践
- AWS 服务的集中管理、部署和版本控制
- 对 AWS 基础设施的可见性和控制

具备以下技能：

- 使用 CloudFormation 一致且安全地部署云资源
- 实施和执行多账户标记策略
- 配置和部署批准的 AWS 服务组合（例如，使用 AWS Service Catalog）
- 将 AWS 资源划分到不同的组进行管理
- 部署 Firewall Manager 以执行策略
- 在 AWS 账户之间安全地共享资源（例如，使用 AWS Resource Access Manager [AWS RAM]）

任务表述 6.3： 评估 AWS 资源的合规性。

掌握以下知识：

- 使用 AWS 服务进行数据分类
- 如何评定、审核和评估 AWS 资源的配置（例如，使用 AWS Config）

具备以下技能：

- 使用 Macie 找出敏感数据
- 创建 AWS Config 规则以检测不合规的 AWS 资源
- 使用 Security Hub 和 AWS Audit Manager 收集和整理证据

任务表述 6.4： 通过架构审核和成本分析找出安全漏洞。

掌握以下知识：

- 用于找出异常的 AWS 成本和使用情况
- 减少攻击面的策略
- AWS Well-Architected Framework

具备以下技能：

- 根据资源使用率和趋势找出异常

- 使用 AWS 服务和工具（例如 AWS Trusted Advisor、AWS Cost Explorer）找出未使用的资源
- 使用 AWS Well-Architected Tool 找出安全漏洞

# 附录

### 考试中可能出现的技术和概念

下表包含考试中可能出现的技术和概念。列表并非详尽无遗，并且可能会发生更改。表中项目的顺序和位置并不表明它们在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)

### 考试范围内的 AWS 服务和功能

注意： 安全性将影响所有 AWS 服务。许多服务未出现在此列表中，因为整体服务超出了范围，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，可能会问及到有关配置 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。列表并非详尽无遗，并且可能会发生更改。AWS 产品/服务的类别与产品/服务的主要功能一致：

管理和监管：

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

联网和内容分发：

- Amazon VPC
  - Network Access Analyzer
  - 网络 ACL
  - 安全组
  - VPC 终端节点

安全性、身份与合规性：

- 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

**超出考试范围的 AWS 服务和功能**

下表列出了超出考试范围的 AWS 服务和功能。列表并非详尽无遗，并且可能会发生更改。与考试的目标工作职责完全无关的 AWS 产品/服务被排除在此列表之外：

区块链：

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

业务应用程序：

- Alexa for Business
- Amazon Chime
- Amazon Chime SDK
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- AWS Supply Chain

- AWS Wickr
- Amazon WorkDocs

终端用户计算：

- Amazon AppStream 2.0

媒体服务：

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

迁移与传输：

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

量子技术：

- Amazon Braket

机器人：

- AWS RoboMaker

卫星：

- AWS Ground Station

**调查问卷**

本考试指南的作用如何？ 请填写我们的调查问卷，告诉我们您的想法。