Exam Guide (SCS-C03)

AWS Certified Security - Specialty

AWS Certified Security - Specialty: Exam Guide (SCS-C03)

Table of Contents

AWS Certified Security - Specialty (SCS-C03)

The AWS Certified Security - Specialty exam is intended for individuals who have a responsibility to secure cloud solutions. The exam validates a candidate's ability to effectively demonstrate knowledge about securing AWS products and services.

Topics

Introduction

The AWS Certified Security - Specialty exam is intended for individuals who have a responsibility to secure cloud solutions. The exam validates a candidate's ability to effectively demonstrate knowledge about securing AWS products and services.

The exam also validates a candidate's ability to complete the following tasks:

- Apply specialized data classifications and AWS data protection mechanisms.
- Implement data-encryption methods and AWS encryption mechanisms.
- Implement AWS mechanisms to follow secure internet protocols.
- Use AWS security services and features to ensure secure production environments.
- Make decisions that account for tradeoffs between cost, security, and deployment complexity to meet a set of application requirements.
- Understand security operations and risks.

Target candidate description

The target candidate should have the equivalent of 3–5 years of experience securing cloud solutions.

Recommended AWS knowledge

The target candidate should have the following AWS knowledge:

- The AWS shared responsibility model and its application
- Managing identity at scale
- Multi-account governance
- Managing software supply chain risks
- Security incident prevention and response strategies
- Vulnerability management in the cloud
- Developing firewall rules at scale for layers 3–7
- Incident root cause analysis
- Experience responding to an audit
- Logging and monitoring strategies
- Data encryption methodologies, both at-rest and in-transit
- Disaster recovery controls, including backup strategies

Job tasks that are out of scope for the target candidate

The following list contains job tasks that the target candidate is not expected to be able to perform. This list is non-exhaustive. These tasks are out of scope for the exam:

- Design cryptographic algorithms
- Analyze traffic on the packet level
- Architect overall cloud deployments
- Manage end-user compute resources
- Train machine learning models

Exam content

Response types

The exam includes one or more of the following question types:

- **Multiple choice:** Has one correct response and three incorrect responses (distractors)
- **Multiple response:** Has two or more correct responses out of five or more response options
- **Ordering:** Has a list of 3–5 responses to complete a specified task. You must select the correct responses and place the responses in the correct order to receive credit for the question.
- **Matching:** Has a list of responses to match with a list of 3–7 prompts. You must match all the pairs correctly to receive credit for the question.

Unanswered questions are scored as incorrect. There is no penalty for guessing. The exam includes 50 questions that affect your score.

Unscored content

The exam includes 15 unscored questions that do not affect your score. AWS collects information about performance on these unscored questions to evaluate these questions for future use as scored questions. These unscored questions are not identified on the exam.

Exam results

The AWS Certified Security - Specialty (SCS-C03) exam has a pass or fail designation. The exam is scored against a minimum standard established by AWS professionals who follow certification industry best practices and guidelines.

Your results for the exam are reported as a scaled score of 100–1,000. The minimum passing score is 750. Your score shows how you performed on the exam as a whole and whether you passed.

Scaled scoring models help equate scores across multiple exam forms that might have slightly different difficulty levels.

Your score report could contain a table of classifications of your performance at each section level. The exam uses a compensatory scoring model, which means that you do not need to achieve a passing score in each section. You need to pass only the overall exam.

Each section of the exam has a specific weighting, so some sections have more questions than other sections have. The table of classifications contains general information that highlights your strengths and weaknesses. Use caution when you interpret section-level feedback.

Content outline

This exam guide includes weightings, content domains, and task statements for the exam. This guide does not provide a comprehensive list of the content on the exam.

The exam has the following content domains and weightings:

- Content Domain 1: Detection (16% of scored content)
- Content Domain 2: Incident Response (14% of scored content)
- Content Domain 3: Infrastructure Security (18% of scored content)
- Content Domain 4: Identity and Access Management (20% of scored content)
- Content Domain 5: Data Protection (18% of scored content)
- Content Domain 6: Security Foundations and Governance (14% of scored content)

Service References

The following sections provide detailed information about AWS services, technologies, and concepts relevant to this certification exam:

- In-Scope AWS Services
- Out-of-Scope AWS Services
- Technologies and Concepts

Content Domain 1: Detection

Tasks

Task 1.1: Design and implement monitoring and alerting solutions for an AWS account or organization

Skills in:

- Skill 1.1.1: Analyze workloads to determine monitoring requirements.
- Skill 1.1.2: Design and implement workload monitoring strategies (for example, by configuring resource health checks).
- Skill 1.1.3: Aggregate security and monitoring events.
- Skill 1.1.4: Create metrics, alerts, and dashboards to detect anomalous data and events (for example, Amazon GuardDuty, Amazon Security Lake, AWS Security Hub, Amazon Macie).
- Skill 1.1.5: Create and manage automations to perform regular assessments and investigations (for example, by deploying AWS Config conformance packs, Security Hub, AWS Systems Manager State Manager).

Task 1.2: Design and implement logging solutions

Skills in:

- Skill 1.2.1: Identify sources for log ingestion and storage based on requirements.
- Skill 1.2.2: Configure logging for AWS services and applications (for example, by configuring an AWS CloudTrail trail for an organization, by creating a dedicated Amazon CloudWatch logging account, by configuring the Amazon CloudWatch Logs agent).
- Skill 1.2.3: Implement log storage and log data lakes (for example, Security Lake) and integrate with third-party security tools.

- Skill 1.2.4: Use AWS services to analyze logs (for example, CloudWatch Logs Insights, Amazon Athena, Security Hub findings).
- Skill 1.2.5: Use AWS services to normalize, parse, and correlate logs (for example, Amazon OpenSearch Service, AWS Lambda, Amazon Managed Grafana).
- Skill 1.2.6: Determine and configure appropriate log sources based on network design, threats, and attacks (for example, VPC Flow Logs, transit gateway flow logs, Amazon Route 53 Resolver logs).

Task 1.3: Troubleshoot security monitoring, logging, and alerting solutions

Skills in:

- Skill 1.3.1: Analyze the functionality, permissions, and configuration of resources (for example, Lambda function logging, Amazon API Gateway logging, health checks, Amazon CloudFront logging).
- Skill 1.3.2: Remediate misconfiguration of resources (for example, by troubleshooting CloudWatch Agent configurations, troubleshooting missing logs).

Content Domain 2: Incident Response

Tasks

Task 2.1: Design and test an incident response plan

Skills in:

- Skill 2.1.1: Design and implement response plans and runbooks to respond to security incidents (for example, Systems Manager OpsCenter, Amazon SageMaker AI notebooks).
- Skill 2.1.2: Use AWS service features and capabilities to configure services to be prepared for incidents (for example, by provisioning access, deploying security tools, minimizing the blast radius, configuring AWS Shield Advanced protections).

- Skill 2.1.3: Recommend procedures to test and validate the effectiveness of an incident response plan (for example, AWS Fault Injection Service, AWS Resilience Hub).
- Skill 2.1.4: Use AWS services to automatically remediate incidents (for example, Systems Manager, Automated Forensics Orchestrator for Amazon EC2, AWS Step Functions, Amazon Application Recovery Controller, Lambda functions).

Task 2.2: Respond to security events

Skills in:

- Skill 2.2.1: Capture and store relevant system and application logs as forensic artifacts.
- Skill 2.2.2: Search and correlate logs for security events across applications and AWS services.
- Skill 2.2.3: Validate findings from AWS security services to assess the scope and impact of an event.
- Skill 2.2.4: Respond to affected resources by containing and eradicating threats, and recover resources (for example, by implementing network containment controls, restoring backups).
- Skill 2.2.5: Describe methods to conduct root cause analysis (for example, Amazon Detective).

Content Domain 3: Infrastructure Security

Tasks

Task 3.1: Design, implement, and troubleshoot security controls for network edge services

Skills in:

- Skill 3.1.1: Define and select edge security strategies based on anticipated threats and attacks.
- Skill 3.1.2: Implement appropriate network edge protection (for example, CloudFront headers, AWS WAF, AWS IoT policies, protecting against OWASP Top 10 threats, Amazon S3 cross-origin resource sharing [CORS], Shield Advanced).

- Skill 3.1.3: Design and implement AWS edge controls and rules based on requirements (for example, geography, geolocation, rate limiting, client fingerprinting).
- Skill 3.1.4: Configure integrations with AWS edge services and third-party services (for example, by ingesting data in Open Cybersecurity Schema Framework [OCSF] format, by using third-party WAF rules).

Task 3.2: Design, implement, and troubleshoot security controls for compute workloads

Skills in:

- Skill 3.2.1: Design and implement hardened Amazon EC2 AMIs and container images to secure compute workloads and embed security controls (for example, Systems Manager, EC2 Image Builder).
- Skill 3.2.2: Apply instance profiles, service roles, and execution roles appropriately to authorize compute workloads.
- Skill 3.2.3: Scan compute resources for known vulnerabilities (for example, scan container images and Lambda functions by using Amazon Inspector, monitor compute runtimes by using GuardDuty).
- Skill 3.2.4: Deploy patches across compute resources to maintain secure and compliant environments by automating update processes and by integrating continuous validation (for example, Systems Manager Patch Manager, Amazon Inspector).
- Skill 3.2.5: Configure secure administrative access to compute resources (for example, Systems Manager Session Manager, EC2 Instance Connect).
- Skill 3.2.6: Configure security tools to discover and remediate vulnerabilities within a pipeline (for example, Amazon Q Developer, Amazon CodeGuru Security).
- Skill 3.2.7: Implement protections and guardrails for generative AI applications (for example, by applying GenAI OWASP Top 10 for LLM Applications protections).

Task 3.3: Design and troubleshoot network security controls

Skills in:

- Skill 3.3.1: Design and troubleshoot appropriate network controls to permit or prevent network traffic as required (for example, security groups, network ACLs, AWS Network Firewall).

- Skill 3.3.2: Design secure connectivity between hybrid and multi-cloud networks (for example, AWS Site-to-Site VPN, AWS Direct Connect, MAC Security [MACsec]).
- Skill 3.3.3: Determine and configure security workload requirements for communication between hybrid environments and AWS (for example, by using AWS Verified Access).
- Skill 3.3.4: Design network segmentation based on security requirements (for example, north/south and east/west traffic protections, isolated subnets).
- Skill 3.3.5: Identify unnecessary network access (for example, AWS Verified Access, Network Access Analyzer, Amazon Inspector network reachability findings).

Content Domain 4: Identity and Access Management

Tasks

Task 4.1: Design, implement, and troubleshoot authentication strategies

Skills in:

- Skill 4.1.1: Design and establish identity solutions for human, application, and system authentication (for example, AWS IAM Identity Center, Amazon Cognito, multi-factor authentication [MFA], identity provider [IdP] integration).
- Skill 4.1.2: Configure mechanisms to issue temporary credentials (for example, AWS STS, Amazon S3 presigned URLs).
- Skill 4.1.3: Troubleshooting authentication issues (for example, CloudTrail, Amazon Cognito, IAM Identity Center permission sets, AWS Directory Service).

Task 4.2: Design, implement, and troubleshoot authorization strategies

Skills in:

- Skill 4.2.1: Design and evaluate authorization controls for human, application, and system access (for example, Amazon Verified Permissions, IAM paths, IAM Roles Anywhere, resource policies for cross-account access, IAM role trust policies).

- Skill 4.2.2: Design attribute-based access control (ABAC) and role-based access control (RBAC) strategies (for example, by configuring resource access based on tags or attributes).
- Skill 4.2.3: Design, interpret, and implement IAM policies by following the principle of least privilege (for example, permission boundaries, session policies).
- Skill 4.2.4: Analyze authorization failures to determine causes or effects (for example, IAM Policy Simulator, IAM Access Analyzer).
- Skill 4.2.5: Investigate and correct unintended permissions, authorizations, or privileges granted to a resource, service, or entity (for example, IAM Access Analyzer).

Content Domain 5: Data Protection

Tasks

- Task 5.1: Design and implement controls for data in transit
- Task 5.2: Design and implement controls for data at rest
- Task 5.3: Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials

Task 5.1: Design and implement controls for data in transit

Skills in:

- Skill 5.1.1: Design and configure mechanisms to require encryption when connecting to connect to resources (for example, by configuring Elastic Load Balancing [ELB] security policies, by enforcing TLS configurations).
- Skill 5.1.2: Design and configure mechanisms for secure and private access to resources (for example, AWS PrivateLink, VPC endpoints, AWS Client VPN, AWS Verified Access).
- Skill 5.1.3: Design and configure inter-resource encryption in transit (for example, inter-node encryption configurations for Amazon EMR, Amazon EKS, SageMaker AI, Nitro encryption).

Task 5.2: Design and implement controls for data at rest

Skills in:

- Skill 5.2.1: Design, implement, and configure data encryption at rest based on specific requirements (for example, by selecting the appropriate encryption key service such as AWS

CloudHSM or AWS KMS or by selecting the appropriate encryption type such as client-side encryption or server-side encryption).

- Skill 5.2.2: Design and configure mechanisms to protect data integrity (for example, S3 Object Lock, S3 Glacier Vault Lock, versioning, digital code signing, file validation).
- Skill 5.2.3: Design automatic lifecycle management and retention solutions for data (for example, S3 Lifecycle policies, S3 Object Lock, Amazon EFS Lifecycle policies, Amazon FSx for Lustre backup policies).
- Skill 5.2.4: Design and configure secure data replication and backup solutions (for example, Amazon Data Lifecycle Manager, AWS Backup, ransomware protection, AWS DataSync).

Task 5.3: Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials

Skills in:

- Skill 5.3.1: Design management and rotation of credentials and secrets (for example, AWS Secrets Manager).
- Skill 5.3.2: Manage and use imported key material (for example, by managing and rotating imported key material, by managing and configuring external key stores).
- Skill 5.3.3: Describe the differences between imported key material and AWS generated key material.
- Skill 5.3.4: Mask sensitive data (for example, CloudWatch Logs data protection policies, Amazon SNS message data protection).
- Skill 5.3.5: Create and manage encryption keys and certificates across a single AWS Region or multiple Regions (for example, AWS KMS customer managed AWS KMS keys, AWS Private Certificate Authority).

Content Domain 6: Security Foundations and Governance

Tasks

Task 6.1: Develop a strategy to centrally deploy and manage AWS accounts

Skills in:

- Skill 6.1.1: Deploy and configure organizations by using AWS Organizations.
- Skill 6.1.2: Implement and manage AWS Control Tower in new and existing environments, and deploy optional and custom controls.
- Skill 6.1.3: Implement organization policies to manage permissions (for example, SCPs, RCPs, AI service opt-out policies, declarative policies).
- Skill 6.1.4: Centrally manage security services (for example, delegated administrator accounts).
- Skill 6.1.5: Manage AWS account root user credentials (for example, by centralizing root access for member accounts, managing MFA, designing break-glass procedures).

Task 6.2: Implement a secure and consistent deployment strategy for cloud resources

Skills in:

- Skill 6.2.1: Use infrastructure as code (IaC) to deploy cloud resources consistently and securely across accounts (for example, CloudFormation stack sets, third-party IaC tools, CloudFormation Guard, cfn-lint).
- Skill 6.2.2: Use tags to organize AWS resources into groups for management (for example, by grouping by department, cost center, environment).
- Skill 6.2.3: Deploy and enforce policies and configurations from a central source (for example, AWS Firewall Manager).
- Skill 6.2.4: Securely share resources across AWS accounts (for example, AWS Service Catalog, AWS Resource Access Manager [AWS RAM]).

Task 6.3: Evaluate the compliance of AWS resources

Skills in:

- Skill 6.3.1: Create or enable rules to detect and remediate noncompliant AWS resources and to send notifications (for example, by using AWS Config to aggregate alerts and remediate non-compliant resources, Security Hub).
- Skill 6.3.2: Use AWS audit services to collect and organize evidence (for example, AWS Audit Manager, AWS Artifact).
- Skill 6.3.3: Use AWS services to evaluate architecture for compliance with AWS security best practices (for example, AWS Well-Architected Framework tool).

In-scope AWS services and features

In-scope AWS services and features

Note: Security affects all AWS services. Many services do not appear in this list because the overall service is out of scope, but the security aspects of the service are in scope. For example, a candidate for this exam would not be asked about the steps to set up replication for an S3 bucket. However, the candidate might be asked about configuring an S3 bucket policy.

The following list contains AWS services and features that are in scope for the exam. This list is non-exhaustive and is subject to change. AWS offerings appear in categories that align with the offerings' primary functions:

Topics

- Analytics
- Application Integration
- Compute
- Developer Tools
- Internet of Things
- Machine Learning
- Management and Governance
- Networking and Content Delivery
- Security, Identity, and Compliance
- Storage and Data Management

Analytics

- Amazon Athena
- Amazon OpenSearch Service

Application Integration

- Amazon SNS
- AWS Step Functions

Compute

- Amazon API Gateway
- Amazon EC2 (including EC2 Image Builder, EC2 Instance Connect)
- Amazon EKS
- Amazon EMR
- AWS Lambda
- Amazon Data Lifecycle Manager

Developer Tools

- AWS Fault Injection Service

Internet of Things

- AWS IoT Core

Machine Learning

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

- Amazon SageMaker AI

Management and Governance

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- AWS Resilience Hub
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor
- AWS User Notifications
- AWS Well-Architected Tool

Networking and Content Delivery

- Amazon Application Recovery Controller
- Amazon VPC
  - Network Access Analyzer
  - Network ACLs
  - Security groups
  - VPC endpoints
  - AWS Site-to-Site VPN
  - Flow Logs
  - VPC Endpoints

  - AWS Verified Access
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53 (including Route 53 Resolver DNS Firewall)
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- Network Access Analyzer
- AWS Transit Gateway

Security, Identity, and Compliance

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Automated Forensics Orchestrator for Amazon EC2
- 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

Storage and Data Management

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon EFS (including EFS Lifecycle policies)
- Amazon FSx for Lustre

Out-of-scope AWS services and features

The following list contains AWS services and features that are out of scope for the exam. This list is non-exhaustive and is subject to change. AWS offerings that are entirely unrelated to the target job roles for the exam are excluded from this list:

Topics

- Application Integration
- Security, Identity, and Compliance

Application Integration

- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)

Security, Identity, and Compliance

- AWS Payment Cryptography

Technologies and Concepts

The following list contains technologies and concepts that might appear on the exam. This list is non-exhaustive and is subject to change. The order and placement of the items in this list is no indication of their relative weight or importance on the exam:

- AWS CLI
- AWS SDKs
- AWS Management Console
- Secure remote access
- Certificate management
- Infrastructure as code (IaC)

Appendix: Comparison of SCS-C02 and SCS-C03

Side-by-side comparison

The following table shows the domains and the percentage of scored questions in each domain for the SCS-C02 exam (in use until December 1, 2025) and the SCS-C03 exam (in use beginning December 2, 2025).

SCS-C02 Domain	SCS-C03 Domain
Domain 1: Threat Detection and Incident Response (14%)	Content Domain 1: Detection (16% of scored content)
Domain 2: Security Logging and Monitoring (18%)	Content Domain 2: Incident Response (14%)
Domain 3: Infrastructure Security (20%)	Content Domain 3: Infrastructure Security (18%)
Domain 4: Identity and Access Management (16%)	Content Domain 4: Identity and Access Management (20%)
Domain 5: Data Protection (18%)	Content Domain 5: Data Protection (18%)

SCS-C02 Domain	SCS-C03 Domain
Domain 6: Management and Security Governance (14%)	Content Domain 6: Security Foundations and Governance (14%)

Additions of content for SCS-C03

In Task 2.2.3, the following content was added:

- 2.2.3 Validate findings from AWS security services to assess the scope and impact of an event.

In Task 3.1.4, the following content was added:

- 3.1.4 Configure integrations with AWS edge services and third-party services (for example, by ingesting data in Open Cybersecurity Schema Framework [OCSF] format, by using third-party WAF rules).

In Task 3.2.7, the following content was added:

- 3.2.7 Implement protections and guardrails for generative AI applications (for example, by applying GenAI OWASP Top 10 for LLM Applications protections).

In Task 5.1.3, the following content was added:

- 5.1.3 Design and configure inter-resource encryption in-transit (for example, inter-node encryption configurations for Amazon EMR, Amazon Elastic Kubernetes Service [Amazon EKS], SageMaker AI, Nitro encryption).

In Task 5.3.3, the following content was added:

- 5.3.3 Describe the differences between imported key material and AWS generated key material.

In Task 5.3.4, the following content was added:

- 5.3.4 Mask sensitive data (for example, CloudWatch Logs data protection policies, Amazon Simple Notification Service [Amazon SNS] message data protection).

In Task 5.3.5, the following content was added:

- 5.3.5 Create and manage encryption keys and certificates across a single AWS Region or multiple Regions (for example, AWS KMS customer managed AWS KMS keys, AWS Private Certificate Authority).

Deletions of content for SCS-C03

In Task 6.4, the following content was removed:

- Identify security gaps through architectural reviews and cost analysis.

In Task 1.1, the following content was removed:

- AWS Security Finding Format (ASFF)

In Task 1.3, the following content was removed:

- AWS Security Incident Response Guide

In Task 2.5 the following content was removed:

- Log format and components (for example, CloudTrail logs)

In Task 3.3, the following content was removed:

- Host-based security (for example, firewalls, hardening)
- Activating host-based security mechanisms (for example, host-based firewalls)

In Task 3.4, the following content was removed:

- How to analyze reachability (for example, by using VPC Reachability Analyzer and Amazon Inspector)
- Fundamental TCP/IP networking concepts (for example, UDP compared with TCP, ports, Open Systems Interconnection [OSI] model, network operating system utilities)

- Identifying, interpreting, and prioritizing problems in network connectivity (for example, by using Amazon Inspector Network Reachability)

In Task 4.2, the following content was removed:

- Components and impact of a policy (for example, Principal, Action, Resource, Condition)

In Task 5.1, the following content was removed:

- TLS concepts
- Designing cross-Region networking by using private VIFs and public VIFs

In Task 5.2, the following content was removed:

- Configure S3 static website hosting.

Recategorizations of content for SCS-C03

The following major content reorganizations have occurred in the transition from SCS-C02 to SCS-C03:

SCS-C03 Domains 1 and 2 have been restructured:

- "Threat Detection and Incident Response" and "Security Logging and Monitoring" are now:
  - Domain 1: Detection
  - Domain 2: Incident Response

Domain 6 has been renamed for SCS-C03:

- From "Management and Security Governance" to "Security Foundations and Governance"

The following task statements have been recategorized:

SCS-C02 Task Statement 1.1 is mapped to the following tasks in SCS-C03:

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.
- 1.2 Design and implement logging.

- 2.1 Design and test an incident response plan.
- 2.2 Respond to security events.

SCS-C02 Task Statement 1.2 is mapped to the following tasks in SCS-C03:

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.
- 1.2 Design and implement logging.

SCS-C02 Task Statement 1.3 is mapped to the following tasks in SCS-C03:

- 2.1 Design and test an incident response plan.
- 2.2 Respond to security events.

SCS-C02 Task Statement 2.1 is mapped to the following tasks in SCS-C03:

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.

SCS-C02 Task Statement 2.2 is mapped to the following tasks in SCS-C03:

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.
- 1.2 Design and implement logging.
- 1.3 Troubleshoot security monitoring, logging and alerting.

SCS-C02 Task Statement 2.3 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.

SCS-C02 Task Statement 2.4 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.
- 1.3 Troubleshoot security monitoring, logging and alerting.

SCS-C02 Task Statement 2.5 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.

SCS-C02 Task Statement 3.1 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.
- 3.1 Design, implement, and troubleshoot security controls for network edge services.

SCS-C02 Task Statement 3.2 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.
- 3.3 Design and troubleshoot network security controls.
- 5.1 Design and implement controls for data in transit.
- 6.2 Implement a secure and consistent deployment strategy for cloud resources.

SCS-C02 Task Statement 3.3 is mapped to the following tasks in SCS-C03:

- 3.2 Design, implement, and troubleshoot security controls for compute workloads.
- 5.3 Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials.

SCS-C02 Task Statement 3.4 is mapped to the following tasks in SCS-C03:

- 1.2 Design and implement logging.
- 3.3 Design and troubleshoot network security controls.

SCS-C02 Task Statement 4.1 is mapped to the following tasks in SCS-C03:

- 4.1 Design, implement, and troubleshoot authentication strategies

SCS-C02 Task Statement 4.2 is mapped to the following tasks in SCS-C03:

- 4.2 Design, implement, and troubleshoot authorization strategies

SCS-C02 Task Statement 5.1 is mapped to the following tasks in SCS-C03:

- 3.2 Design, implement, and troubleshoot security controls for compute workloads.
- 3.3 Design and troubleshoot network security controls.

- 5.1 Design and implement controls for data in transit.

SCS-C02 Task Statement 5.2 is mapped to the following tasks in SCS-C03:

- 4.2 Design, implement, and troubleshoot authorization strategies
- 5.2 Design and implement controls for data at rest.

SCS-C02 Task Statement 5.3 is mapped to the following tasks in SCS-C03:

- 5.2 Design and implement controls for data at rest.

SCS-C02 Task Statement 5.4 is mapped to the following tasks in SCS-C03:

- 5.2 Design and implement controls for data at rest.
- 5.3 Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials.

SCS-C02 Task Statement 6.1 is mapped to the following tasks in SCS-C03:

- 4.2 Design, implement, and troubleshoot authorization strategies
- 6.1 Develop a strategy to centrally deploy and manage AWS accounts.

SCS-C02 Task Statement 6.2 is mapped to the following tasks in SCS-C03:

- 6.2 Implement a secure and consistent deployment strategy for cloud resources.

SCS-C02 Task Statement 6.3 is mapped to the following tasks in SCS-C03:

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.
- 5.2 Design and implement controls for data at rest.
- 6.3 Evaluate the compliance of AWS resources.

SCS-C02 Task Statement 6.4 is mapped to the following tasks in SCS-C03:

- 2.1 Design and test an incident response plan.

- 1.1 Design and implement monitoring and alerting for an AWS account or organization.
- 6.3 Evaluate the compliance of AWS resources.

Revisions

AWS exam guides are periodically reviewed and updated to ensure that our certification exams test skills and AWS services and features that are relevant for the job role(s) that a certification is designed to target. Exam guide updates will be published approximately one month before updates will be reflected on your exam.

Topics

- Change History

Change History

Version	Publication date
1.0	March 26, 2026

Survey

How useful was this exam guide? Let us know by taking our survey.