AWS SCS-C02

AWS Security Specialty Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

SCS-C02

AWS Certified Security - Specialty

65 Questions Exam – 750 / 1000 Cut Score – Duration of 170 minutes

Table of Contents:

Discover More about the SCS-C02 Certification

Are you interested in passing the AWS SCS-C02 exam? First discover, who benefits from the SCS-C02 certification. The SCS-C02 is suitable for a candidate if he wants to learn about Specialty. Passing the SCS-C02 exam earns you the AWS Certified Security - Specialty title.

While preparing for the SCS-C02 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SCS-C02 PDF contains some of the most valuable preparation tips and the details and instant access to useful SCS-C02 study materials **just at one click**.

AWS SCS-C02 Security Specialty Certification Details:

Exam Name	AWS Certified Security - Specialty (Security Specialty)
Exam Code	SCS-C02
Exam Price	$300 USD
Duration	170 minutes
Number of Questions	65
Passing Score	750 / 1000
Recommended Training / Books	**AWS Security Fundamentals (Second Edition)** **Security Engineering on AWS** **AWS Cloud Quest Security Role**
Schedule Exam	**PEARSON VUE**
Sample Questions	**AWS SCS-C02 Sample Questions**
Recommended Practice	**AWS Certified Security - Specialty Practice Test**

SCS-C02 Syllabus:

Section	Objectives
Threat Detection and Incident Response - 14%	
Design and	- Knowledge of:

Section	Objectives
implement an incident response plan.	• AWS best practices for incident response • Cloud incidents • Roles and responsibilities in the incident response plan • AWS Security Finding Format (ASFF) - Skills in: • Implementing credential invalidation and rotation strategies in response to compromises (for example, by using AWS Identity and Access Management [IAM] and AWS Secrets Manager) • Isolating AWS resources • Designing and implementing playbooks and runbooks for responses to security incidents • Deploying security services (for example, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer) • Configuring integrations with native AWS services and third-party services (for example, by using Amazon EventBridge and the ASFF)
Detect security threats and anomalies by using AWS services.	- Knowledge of: • AWS managed security services that detect threats • Anomaly and correlation techniques to join data across services • Visualizations to identify anomalies • Strategies to centralize security findings - Skills in: • Evaluating findings from security services (for example, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer) • Searching and correlating security threats across AWS services (for example, by using Detective) • Performing queries to validate security events (for example, by using Amazon Athena) • Creating metric filters and dashboards to detect anomalous activity (for example, by using Amazon CloudWatch)
Respond to compromised resources and workloads.	- Knowledge of: • AWS Security Incident Response Guide • Resource isolation mechanisms

Section	Objectives
	• Techniques for root cause analysis • Data capture mechanisms • Log analysis for event validation - Skills in: • Automating remediation by using AWS services (for example, AWS Lambda, AWS Step Functions, EventBridge, AWS Systems Manager runbooks, Security Hub, AWS Config) • Responding to compromised resources (for example, by isolating Amazon EC2 instances) • Investigating and analyzing to conduct root cause analysis (for example, by using Detective) • Capturing relevant forensics data from a compromised resource (for example, Amazon Elastic Block Store [Amazon EBS] volume snapshots, memory dump) • Querying logs in Amazon S3 for contextual information related to security events (for example, by using Athena) • Protecting and preserving forensic artifacts (for example, by using S3 Object Lock, isolated forensic accounts, S3 Lifecycle, and S3 replication) • Preparing services for incidents and recovering services after incidents
Security Logging and Monitoring - 18%	
Design and implement monitoring and alerting to address security events.	- Knowledge of: • AWS services that monitor events and provide alarms (for example, CloudWatch, EventBridge) • AWS services that automate alerting (for example, Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub) • Tools that monitor metrics and baselines (for example, GuardDuty, Systems Manager) - Skills in: • Analyzing architectures to identify monitoring requirements and sources of data for security monitoring • Analyzing environments and workloads to determine monitoring requirements • Designing environment monitoring and workload monitoring based on business and security requirements • Setting up automated tools and scripts to perform regular audits (for example, by creating custom insights in Security Hub)

Section	Objectives
	• Defining the metrics and thresholds that generate alerts
Troubleshoot security monitoring and alerting.	- Knowledge of: • Configuration of monitoring services (for example, Security Hub) • Relevant data that indicates security events - Skills in: • Analyzing the service functionality, permissions, and configuration of resources after an event that did not provide visibility or alerting • Analyzing and remediating the configuration of a custom application that is not reporting its statistics • Evaluating logging and monitoring services for alignment with security requirements
Design and implement a logging solution.	- Knowledge of: • AWS services and features that provide logging capabilities (for example, VPC Flow Logs, DNS logs, AWS CloudTrail, Amazon CloudWatch Logs) • Attributes of logging capabilities (for example, log levels, type, verbosity) • Log destinations and lifecycle management (for example, retention period) - Skills in: • Configuring logging for services and applications • Identifying logging requirements and sources for log ingestion • Implementing log storage and lifecycle management according to AWS best practices and organizational requirements
Troubleshoot logging solutions.	- Knowledge of: • Capabilities and use cases of AWS services that provide data sources (for example, log level, type, verbosity, cadence, timeliness, immutability) • AWS services and features that provide logging capabilities (for example, VPC Flow Logs, DNS logs, CloudTrail, CloudWatch Logs) • Access permissions that are necessary for logging - Skills in: • Identifying misconfiguration and determining remediation steps for absent access permissions that are

Section	Objectives
	necessary for logging (for example, by managing read/write permissions, S3 bucket permissions, public access, and integrity) • Determining the cause of missing logs and performing remediation steps
Design a log analysis solution.	- Knowledge of: • Services and tools to analyze captured logs (for example, Athena, CloudWatch Logs filter) • Log analysis features of AWS services (for example, CloudWatch Logs Insights, CloudTrail Insights, Security Hub insights) • Log format and components (for example, CloudTrail logs) - Skills in: • Identifying patterns in logs to indicate anomalies and known threats • Normalizing, parsing, and correlating logs
Infrastructure Security - 20%	
Design and implement security controls for edge services.	- Knowledge of: • Security features on edge services (for example, AWS WAF, load balancers, Amazon Route 53, Amazon CloudFront, AWS Shield) • Common attacks, threats, and exploits (for example, Open Web Application Security Project [OWASP] Top 10, DDoS) • Layered web application architecture - Skills in: • Defining edge security strategies for common use cases (for example, public website, serverless app, mobile app backend) • Selecting appropriate edge services based on anticipated threats and attacks (for example, OWASP Top 10, DDoS) • Selecting appropriate protections based on anticipated vulnerabilities and risks (for example, vulnerable software, applications, libraries) • Defining layers of defense by combining edge security services (for example, CloudFront with AWS WAF and load balancers) • Applying restrictions at the edge based on various criteria (for example, geography, geolocation, rate limit)

Section	Objectives
	• Activating logs, metrics, and monitoring around edge services to indicate attacks
Design and implement network security controls.	- Knowledge of: • VPC security mechanisms (for example, security groups, network ACLs, AWS Network Firewall) • Inter-VPC connectivity (for example, AWS Transit Gateway, VPC endpoints) • Security telemetry sources (for example, Traffic Mirroring, VPC Flow Logs) • VPN technology, terminology, and usage • On-premises connectivity options (for example, AWS VPN, AWS Direct Connect) - Skills in: • Implementing network segmentation based on security requirements (for example, public subnets, private subnets, sensitive VPCs, on-premises connectivity) • Designing network controls to permit or prevent network traffic as required (for example, by using security groups, network ACLs, and Network Firewall) • Designing network flows to keep data off the public internet (for example, by using Transit Gateway, VPC endpoints, and Lambda in VPCs) • Determining which telemetry sources to monitor based on network design, threats, and attacks (for example, load balancer logs, VPC Flow Logs, Traffic Mirroring) • Determining redundancy and security workload requirements for communication between on-premises environments and the AWS Cloud (for example, by using AWS VPN, AWS VPN over Direct Connect, and MACsec) • Identifying and removing unnecessary network access • Managing network configurations as requirements change (for example, by using AWS Firewall Manager)
Design and implement security controls for compute workloads.	- Knowledge of: • Provisioning and maintenance of EC2 instances (for example, patching, inspecting, creation of snapshots and AMIs, use of EC2 Image Builder) • IAM instance roles and IAM service roles • Services that scan for vulnerabilities in compute workloads (for example, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR]) • Host-based security (for example, firewalls, hardening)

Section	Objectives
	- Skills in: • Creating hardened EC2 AMIs • Applying instance roles and service roles as appropriate to authorize compute workloads • Scanning EC2 instances and container images for known vulnerabilities • Applying patches across a fleet of EC2 instances or container images • Activating host-based security mechanisms (for example, host-based firewalls) • Analyzing Amazon Inspector findings and determining appropriate mitigation techniques • Passing secrets and credentials securely to compute workloads
Troubleshoot network security.	- Knowledge of: • 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) • How to read relevant log sources (for example, Route 53 logs, AWS WAF logs, VPC Flow Logs) - Skills in: • Identifying, interpreting, and prioritizing problems in network connectivity (for example, by using Amazon Inspector Network Reachability) • Determining solutions to produce desired network behavior • Analyzing log sources to identify problems • Capturing traffic samples for problem analysis (for example, by using Traffic Mirroring)
Identity and Access Management - 16%	
Design, implement, and troubleshoot authentication for AWS resources.	- Knowledge of: • Methods and services for creating and managing identities (for example, federation, identity providers, AWS IAM Identity Center [AWS Single Sign-On], Amazon Cognito) • Long-term and temporary credentialing mechanisms • How to troubleshoot authentication issues (for example,

Section	Objectives
	by using CloudTrail, IAM Access Advisor, and IAM policy simulator) - Skills in: • Establishing identity through an authentication system, based on requirements • Setting up multi-factor authentication (MFA) • Determining when to use AWS Security Token Service (AWS STS) to issue temporary credentials
Design, implement, and troubleshoot authorization for AWS resources.	- Knowledge of: • Different IAM policies (for example, managed policies, inline policies, identity-based policies, resource-based policies, session control policies) • Components and impact of a policy (for example, Principal, Action, Resource, Condition) • How to troubleshoot authorization issues (for example, by using CloudTrail, IAM Access Advisor, and IAM policy simulator) - Skills in: • Constructing attribute-based access control (ABAC) and role-based access control (RBAC) strategies • Evaluating IAM policy types for given requirements and workloads • Interpreting an IAM policy's effect on environments and workloads • Applying the principle of least privilege across an environment • Enforcing proper separation of duties • Analyzing access or authorization errors to determine cause or effect • Investigating unintended permissions, authorization, or privileges granted to a resource, service, or entity
Data Protection - 18%	
Design and implement controls that provide confidentiality and integrity for data in transit.	- Knowledge of: • TLS concepts • VPN concepts (for example, IPsec) • Secure remote access methods (for example, SSH, RDP over Systems Manager Session Manager) • Systems Manager Session Manager concepts • How TLS certificates work with various network services

Section	Objectives
	and resources (for example, CloudFront, load balancers) - Skills in: • Designing secure connectivity between AWS and on-premises networks (for example, by using Direct Connect and VPN gateways) • Designing mechanisms to require encryption when connecting to resources (for example, Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, load balancers, Amazon Elastic File System [Amazon EFS], Amazon API Gateway) • Requiring TLS for AWS API calls (for example, with Amazon S3) • Designing mechanisms to forward traffic over secure connections (for example, by using Systems Manager and EC2 Instance Connect) • Designing cross-Region networking by using private VIFs and public VIFs
Design and implement controls that provide confidentiality and integrity for data at rest.	- Knowledge of: • Encryption technique selection (for example, client-side, server-side, symmetric, asymmetric) • Integrity-checking techniques (for example, hashing algorithms, digital signatures) • Resource policies (for example, for DynamoDB, Amazon S3, and AWS Key Management Service [AWS KMS]) • IAM roles and policies - Skills in: • Designing resource policies to restrict access to authorized users (for example, S3 bucket policies, DynamoDB policies) • Designing mechanisms to prevent unauthorized public access (for example, S3 Block Public Access, prevention of public snapshots and public AMIs) • Configuring services to activate encryption of data at rest (for example, Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS) • Designing mechanisms to protect data integrity by preventing modifications (for example, by using S3 Object Lock, KMS key policies, S3 Glacier Vault Lock, and AWS Backup Vault Lock) • Designing encryption at rest by using AWS CloudHSM for relational databases (for example, Amazon RDS, RDS Custom, databases on EC2 instances)

Section	Objectives
	• Choosing encryption techniques based on business requirements
Design and implement controls to manage the lifecycle of data at rest.	- Knowledge of: • Lifecycle policies • Data retention standards - Skills in: • Designing S3 Lifecycle mechanisms to retain data for required retention periods (for example, S3 Object Lock, S3 Glacier Vault Lock, S3 Lifecycle policy) • Designing automatic lifecycle management for AWS services and resources (for example, Amazon S3, EBS volume snapshots, RDS volume snapshots, AMIs, container images, CloudWatch log groups, Amazon Data Lifecycle Manager • Establishing schedules and retention for AWS Backup across AWS services
Design and implement controls to protect credentials, secrets, and cryptographic key materials.	- Knowledge of: • Secrets Manager • Systems Manager Parameter Store • Usage and management of symmetric keys and asymmetric keys (for example, AWS KMS) - Skills in: • Designing management and rotation of secrets for workloads (for example, database access credentials, API keys, IAM access keys, AWS KMS customer managed keys) • Designing KMS key policies to limit key usage to authorized users • Establishing mechanisms to import and remove customer-provided key material
Management and Security Governance - 14%	
Develop a strategy to centrally deploy and manage AWS accounts.	- Knowledge of: • Multi-account strategies • Managed services that allow delegated administration • Policy-defined guardrails • Root account best practices • Cross-account roles

Section	Objectives
	- Skills in: • Deploying and configuring AWS Organizations • Determining when and how to deploy AWS Control Tower (for example, which services must be deactivated for successful deployment) • Implementing SCPs as a technical solution to enforce a policy (for example, limitations on the use of a root account, implementation of controls in AWS Control Tower) • Centrally managing security services and aggregating findings (for example, by using delegated administration and AWS Config aggregators) • Securing AWS account root user credentials
Implement a secure and consistent deployment strategy for cloud resources.	- Knowledge of: • Deployment best practices with infrastructure as code (IaC) (for example, AWS CloudFormation template hardening and drift detection) • Best practices for tagging • Centralized management, deployment, and versioning of AWS services • Visibility and control over AWS infrastructure - Skills in: • Using CloudFormation to deploy cloud resources consistently and securely • Implementing and enforcing multi-account tagging strategies • Configuring and deploying portfolios of approved AWS services (for example, by using AWS Service Catalog) • Organizing AWS resources into different groups for management • Deploying Firewall Manager to enforce policies • Securely sharing resources across AWS accounts (for example, by using AWS Resource Access Manager [AWS RAM])
Evaluate the compliance of AWS resources.	- Knowledge of: • Data classification by using AWS services • How to assess, audit, and evaluate the configurations of AWS resources (for example, by using AWS Config) - Skills in:

Section	Objectives
	• Identifying sensitive data by using Macie • Creating AWS Config rules for detection of noncompliant AWS resources • Collecting and organizing evidence by using Security Hub and AWS Audit Manager
Identify security gaps through architectural reviews and cost analysis.	- Knowledge of: • AWS cost and usage for anomaly identification • Strategies to reduce attack surfaces • AWS Well-Architected Framework - Skills in: • Identifying anomalies based on resource utilization and trends • Identifying unused resources by using AWS services and tools (for example, AWS Trusted Advisor, AWS Cost Explorer) • Using the AWS Well-Architected Tool to identify security gaps

Broaden Your Knowledge with AWS SCS-C02 Sample Questions:

Question: 1

A Security Engineer must ensure that all API calls are collected across all company accounts, and that they are preserved online and are instantly available for analysis for 90 days. For compliance reasons, this data must be restorable for 7 years.

Which steps must be taken to meet the retention needs in a scalable, cost-effective way?

a) Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket with versioning enabled. Set a lifecycle policy to move the data to Amazon Glacier daily, and expire the data after 90 days.
b) Enable AWS CloudTrail logging across all accounts to S3 buckets. Set a lifecycle policy to expire the data in each bucket after 7 years.
c) Enable AWS CloudTrail logging across all accounts to Amazon Glacier. Set a lifecycle policy to expire the data after 7 years.
d) Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket. Set a lifecycle policy to move the data to Amazon Glacier after 90 days, and expire the data after 7 years.

Answer: d

Question: 2

Why is it important to scan network logs?

a) To keep an eye on what the employees on your network are doing.
b) To ensure there are no dropped packets or high latency.
c) To be alerted to unusual traffic entering and exiting your network as a potential security event.
d) To know if access has been made to your private S3 buckets.

Answer: c

Question: 3

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data.

Which solution meets the requirement with the LEAST risk and effort?

a) Use Amazon CloudWatch Logs to capture all logs, write an AWS Lambda function that parses the log file, and move sensitive data to a different log.
b) Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required.
c) Aggregate logs into one file, then use Amazon CloudWatch Logs, and then design two CloudWatch metric filters to filter sensitive data from the logs.
d) Add logic to the application that saves sensitive data logs on the Amazon EC2 instances' local storage, and write a batch script that logs into the Amazon EC2 instances and moves sensitive logs to a secure location.

Answer: b

Question: 4

A Security Engineer has been informed that a user’s access key has been found on GitHub. The Engineer must ensure that this access key cannot continue to be used, and must assess whether the access key was used to perform any unauthorized activities.

Which steps must be taken to perform these tasks?

a) Review the user's IAM permissions and delete any unrecognized or unauthorized resources.
b) Delete the user, review Amazon CloudWatch Logs in all regions, and report the abuse.
c) Delete or rotate the user’s key, review the AWS CloudTrail logs in all regions, and delete any unrecognized or unauthorized resources.
d) Instruct the user to remove the key from the GitHub submission, rotate keys, and re-deploy any instances that were launched.

Answer: c

Question: 5

A Security Engineer must set up security group rules for a three-tier application:

- Presentation tier – Accessed by users over the web, protected by the security group presentation-sg

- Logic tier – RESTful API accessed from the presentation tier through HTTPS, protected by the security group logic-sg

- Data tier – SQL Server database accessed over port 1433 from the logic tier, protected by the security group data-sg

Which combination of the following security group rules will allow the application to be secure and functional?

(Select THREE.)

a) presentation-sg: Allow ports 80 and 443 from 0.0.0.0/0
b) data-sg: Allow port 1433 from presentation-sg
c) data-sg: Allow port 1433 from logic-sg
d) presentation-sg: Allow port 1433 from data-sg
e) logic-sg: Allow port 443 from presentation-sg
f) logic-sg: Allow port 443 from 0.0.0.0/0

Answer: a, c, e

Question: 6

A company decides to place database hosts in its own VPC, and to set up VPC peering to different VPCs containing the application and web tiers. The application servers are unable to connect to the database.

Which network troubleshooting steps should be taken to resolve the issue?

(Select TWO.)

a) Check to see if the application servers are in a private subnet or public subnet.
b) Check the route tables for the application server subnets for routes to the VPC peering connection.
c) Check the NACLs for the database subnets for rules that allow traffic from the internet.
d) Check the database security groups for rules that allow traffic from the application servers.
e) Check to see if the database VPC has an internet gateway

Answer: b, d

Question: 7

A company is hosting a web application on AWS and is using an Amazon S3 bucket to store images. Users should have the ability to read objects in the bucket. A Security Engineer has written the following bucket policy to grant public read access:

```
{
   "ID":"Policy1502987489630",
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1502987487640",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":"arn:aws:s3:::appbucket",
         "Principal":"*"
      }
   ]
}
```

Attempts to read an object, however, receive the error: "Action does not apply to any resource(s) in statement." What should the Engineer do to fix the error?

a) Change the IAM permissions by applying PutBucketPolicy permissions.
b) Verify that the policy has the same name as the bucket name. If not, make it the same.
c) Change the resource section to "arn:aws:s3:::appbucket/*".
d) Add an s3:ListBucket action.

Answer: c

Question: 8

A corporate cloud security policy states that communication between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement?

(Select TWO.)

a) Add the aws:sourceVpce condition to the AWS KMS key policy referencing the company's VPC endpoint ID.
b) Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.
c) Create a VPC endpoint for AWS KMS with private DNS enabled.
d) Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
e) Add the following condition to the AWS KMS key policy: "aws:SourceIp": "10.0.0.0/16".

Answer: a, c

Question: 9

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information.

The Security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.

Which combination of steps would meet the requirements?

(Select TWO.)

a) Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
b) Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
c) Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.
d) Add a bucket policy with aws:SourceIp to allow uploads and downloads from the corporate intranet only.
e) Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: b, c

Question: 10

When testing a new AWS Lambda function that retrieves items from an Amazon DynamoDB table, the Security Engineer notices that the function was not logging any data to Amazon CloudWatch Logs.

The following policy was assigned to the role assumed by the Lambda function:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Dynamo-1234567",
"Action": [
"dynamodb:GetItem"
],
"Effect": "Allow",
"Resource": "*"
}
```

}

Which least-privilege policy addition would allow this function to log properly?

a) {
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:*"
],
"Effect": "Allow"
}
b) {
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogStream"
],
"Effect": "Allow"
}
c) {
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents"
],
"Effect": "Allow"
}
d) {
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:DeleteLogGroup",
"logs:DeleteLogStream",
"logs:getLogEvents",
"logs:PutLogEvents"
],
"Effect": "Allow"
}

Answer: c

Avail the Study Guide to Pass AWS SCS-C02 Security Specialty Exam:

- Find out about the SCS-C02 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **SCS-C02 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the SCS-C02 training. Joining the AWS provided training for SCS-C02 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **SCS-C02 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SCS-C02 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the SCS-C02 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the SCS-C02 Certification

VMExam.Com is here with all the necessary details regarding the SCS-C02 exam. We provide authentic practice tests for the SCS-C02 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on VMExam.Com for rigorous, unlimited two-month attempts on the **SCS-C02 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the AWS Certified Security - Specialty.

Start Online practice of SCS-C02 Exam by visiting URL
https://www.vmexam.com/aws/scs-c02-aws-certified-security-specialty