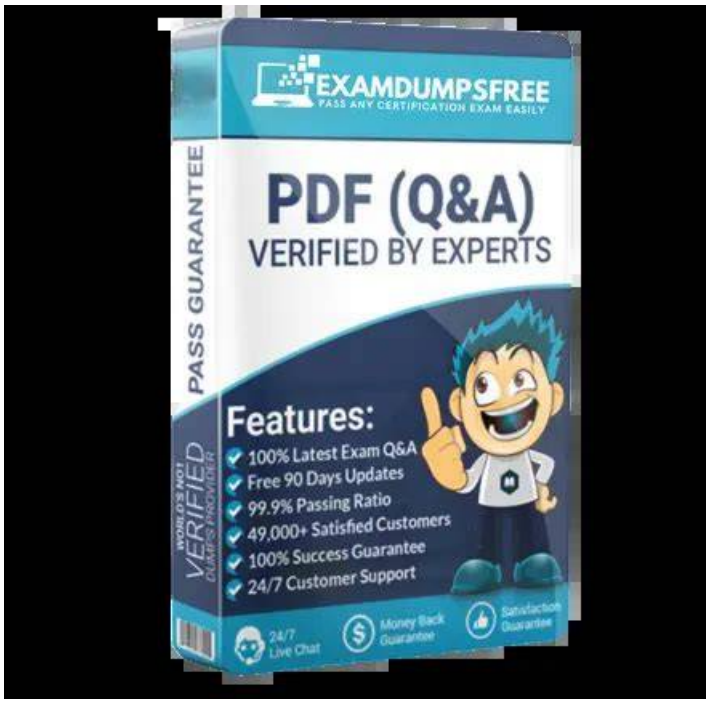
BootcampPDF Composite Test SCS-C02 Price - Obtain Right now



2026 Latest BootcampPDF SCS-C02 PDF Dumps and SCS-C02 Exam Engine Free Share: https://drive.google.com/open?id=1oc6YDX_XDQOh7TxpDDe4XZJ_sRZv6zR0

They all got benefits from SCS-C02 certification and now they are SCS-C02 certification holders. You can also become part of this skilled and qualified community. To do this you just need to pass the Amazon SCS-C02 certification exam. Are you ready for this? Do you want to become a AWS Certified Security - Specialty certified? If your answer is positive then we assure you that you are at the right place. Register yourself for AWS Certified Security - Specialty (SCS-C02) certification exam and download the BootcampPDF SCS-C02 exam practice questions and start preparation right now.

Amazon SCS-C02 Exam Overview:

Certification Vendor:	Amazon Web Services (AWS)
Exam Name:	AWS Certified Security - Specialty
Exam Number:	SCS-C02
Related Certifications:	AWS Certified Cloud Practitioner AWS Certified Solutions Architect - Associate AWS Certified Security - Associate
Certificate Validity Period:	3 years
Real Exam Qty:	65
Available Languages:	English, Japanese, Korean, Portuguese (Brazil), Simplified Chinese, Spanish (Latin America)
Passing Score:	750 (scaled score 100–1000)
Exam Duration:	170 minutes
Exam Price:	USD 300
Exam Format:	Multiple choice, Multiple response, Scenario-based questions
Recommended Training:	AWS Certified Security - Specialty Exam Prep Plan AWS Security Fundamentals
Exam Registration:	Pearson VUE Registration AWS Certification Registration
Sample Questions:	Amazon SCS-C02 Sample Questions
Exam Way:	Online proctored exam or onsite at Pearson VUE test centers

Pre Condition:	Recommended: 5+ years of IT security experience, 2+ years of hands-on experience securing AWS workloads; familiarity with AWS core services and security best practices
Official Syllabus URL:	https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/certification/approved/pdfs/docs-security-spec/AWS-Certified-Security-Specialty_Exam-Guide.pdf

>> Composite Test SCS-C02 Price <<

Amazon - The Best SCS-C02 - Composite Test AWS Certified Security - Specialty Price

Once you learn all SCS-C02 questions and answers in the study guide, try BootcampPDF's innovative testing engine for exam like SCS-C02 practice tests. These tests are made on the pattern of the Amazon real exam and thus remain helpful not only for the purpose of revision but also to know the real exam scenario. To ensure excellent score in the exam, BootcampPDF's braindumps are the real feast for all exam candidates. They contain questions and answers on all the core points of your exam syllabus. Most of these questions are likely to appear in the SCS-C02 Real Exam.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.
Topic 2	• Security Logging and Monitoring: This topic prepares AWS Security specialists to design and implement robust monitoring and alerting systems for addressing security events. It emphasizes troubleshooting logging solutions and analyzing logs to enhance threat visibility.
Topic 3	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.
Topic 4	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.

Amazon AWS Certified Security - Specialty Sample Questions (Q207-Q212):

NEW QUESTION # 207
Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.
Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC.
These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.
The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.
How will the security engineer be able to comply with these requirements?

- A. Remove the existing NAT gateway. Create a new NAT gateway that only the application server subnets can use.
- B. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

- C. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.
- D. Configure the DB instance's inbound network ACL to deny traffic from the security group ID of the NAT gateway.

Answer: C

Explanation:
Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

NEW QUESTION # 208
A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.
Which solution will meet these requirements?

- A. Set up GuardDuty to send notifications to AWS CloudTrail with two targets in CloudTrail. From CloudTrail, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings.
  Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for CloudTrail. Use event pattern matching with a CloudTrail event rule to send only High severity findings in the alerts.
- B. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.
- C. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.
- D. Set up GuardDuty to send notifications to an Amazon CloudWatch alarm with two targets in CloudWatch. From CloudWatch, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for the CloudWatch alarm. Use event pattern matching with an Amazon EventBridge event rule to send only High severity findings in the alerts.

Answer: C

NEW QUESTION # 209
A company operates a web application that runs on Amazon EC2 instances. The application listens on port 80 and port 443. The company uses an Application Load Balancer (ALB) with AWS WAF to terminate SSL and to forward traffic to the application instances only on port 80.
The ALB is in public subnets that are associated with a network ACL that is named NACL1. The application instances are in dedicated private subnets that are associated with a network ACL that is named NACL2. An Amazon RDS for PostgreSQL DB instance that uses port 5432 is in a dedicated private subnet that is associated with a network ACL that is named NACL3. All the network ACLs currently allow all inbound and outbound traffic.
Which set of network ACL changes will increase the security of the application while ensuring functionality?

- A. Make the following changes to NACL3:* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the application instance subnets.* Add a rule that allows outbound traffic on ports 1024-65536 to the application instance subnets.* Remove the default rules that allow all inbound and outbound traffic.
- B. Make the following changes to NACL2:* Add a rule that allows outbound traffic on port 5432 to the CIDR blocks of the RDS subnets.* Remove the default rules that allow all inbound and outbound traffic.
- C. Make the following changes to NACL2:* Add a rule that allows inbound traffic on port 5432 from the CIDR blocks of the RDS subnets.* Add a rule that allows outbound traffic on port 5432 to the RDS subnets.
- D. Make the following changes to NACL3:* Add a rule that allows inbound traffic on port 5432 from NACL2.* Add a rule that allows outbound traffic on ports 1024-65536 to NACL2.* Remove the default rules that allow all inbound and outbound traffic.

Answer: A

Explanation:
For increased security while ensuring functionality, adjusting NACL3 to allow inbound traffic on port 5432 from the CIDR blocks of the application instance subnets, and allowing outbound traffic on ephemeral ports (1024-65536) back to those subnets creates a secure path for database access. Removing default allow-all rules enhances security by implementing the principle of least privilege, ensuring that only necessary traffic is permitted.

NEW QUESTION # 210
A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.
The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized.
Which solution will meet these requirements?

- A. Use KMS key rotation. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.
- B. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Decrypt the data by using a keyring that has the primary key in the multi-keyring.
- C. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
- D. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Answer: C

Explanation:
The correct answer is B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
This answer is correct because data key caching can improve performance, reduce cost, and help the company stay within the service limits of AWS KMS. Data key caching stores data keys and related cryptographic material in a cache, and reuses them for encryption and decryption operations. This reduces the number of requests to AWS KMS endpoints and avoids throttling. The AWS Encryption SDK provides a local cache and a caching cryptographic materials manager (caching CMM) that interacts with the cache and enforces security thresholds that the company can set1.
The other options are incorrect because:
* A. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization. Keyrings are used to generate, encrypt, and decrypt data keys, but they do not cache or reuse them. Using each keyring individually or combining them into a multi-keyring does not reduce the number of requests to AWS KMS endpoints2.
* C. Using KMS key rotation does not address the problem of throttling or cost optimization. Key rotation is a security practice that creates new cryptographic material for a KMS key every year, but it does not affect the data that the KMS key protects. Key rotation does not reduce the number of requests to AWS KMS endpoints, and it might incur additional costs for storing multiple versions of key material3.
* D. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization, as explained in option A. Moreover, using any of the wrapping keys in the multi-keyring
* to decrypt the data is not a valid option, because only one of the wrapping keys can decrypt a given data key. The wrapping key that encrypts a data key is stored in the encrypted data key structure, and only that wrapping key can decrypt it4.
References:
1: Data key caching - AWS Encryption SDK 2: Using keyrings - AWS Encryption SDK 3: Rotating AWS KMS keys - AWS Key Management Service 4: How keyrings work - AWS Encryption SDK

NEW QUESTION # 211
A company used AWS Organizations to set up an environment with multiple AWS accounts. The company's organization currently has two AWS accounts, and the company expects to add more than 50 AWS accounts during the next 12 months The company will require all existing and future AWS accounts to use Amazon GuardDuty. Each existing AWS account has GuardDuty active.
The company reviews GuardDuty findings by logging into each AWS account individually.
The company wants a centralized view of the GuardDuty findings for the existing AWS accounts and any future AWS accounts. The company also must ensure that any new AWS account has GuardDuty automatically turned on.

Which solution will meet these requirements?

- A. D. Enable AWS Security Hub in the organization's management account. Designate the management account as the delegated administrator account for Security Hub. Add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization. Send all Security Hub findings to the organization's GuardDuty account.
- B. Create a new AWS account in the organization. Enable GuardDuty in the new account. Enable AWS Security Hub in each account. Select the option to automatically add new AWS accounts to the organization.
- C. B. Create a new AWS account in the organization. Enable GuardDuty in the new account. Designate the new account as the delegated administrator account for GuardDuty. Configure GuardDuty to add existing accounts as member accounts. Select the option to automatically add new AWS accounts to the organization

Answer: B

Explanation:
For a company using AWS Organizations that requires centralized management and automatic activation of Amazon GuardDuty across all current and future AWS accounts, setting up a delegated administrator account for GuardDuty is the optimal solution. By enabling GuardDuty in a new account and designating it as the delegated administrator, the company can centrally manage GuardDuty findings and automatically enroll new AWS accounts into GuardDuty as they are created within the organization. This approach ensures consistent threat detection and continuous monitoring across all accounts, aligning with best security practices.

NEW QUESTION # 212
.....