

Pass Guaranteed 2026 Unparalleled Amazon SCS-C03: AWS Certified Security - Specialty Valid Study Materials



2026 Latest TestKingFree SCS-C03 PDF Dumps and SCS-C03 Exam Engine Free Share: <https://drive.google.com/open?id=1XMqHBVlbcK-fCh8nwe37zBtrkLWCnByT>

The TestKingFree wants to help students ace the certification exam preparation. To achieve this goal the TestKingFree is offering real, valid, and updated exam questions in three different formats. These Amazon SCS-C03 exam questions formats are PDF file, desktop practice test software, and web-based practice test software. All these three SCS-C03 Exam Practice question formats are easy to use. The SCS-C03 desktop practice test software and web-based practice test software both are the easy-to-use mock AWS Certified Security - Specialty (SCS-C03) exam. These SCS-C03 mock exams are designed to simulate the conditions of a real exam.

The TestKingFree SCS-C03 PDF questions file, desktop practice test software, and web-based practice test software, all these three SCS-C03 practice test questions formats are ready for instant download. Just download any Amazon SCS-C03 Exam Questions format and start this journey with confidence.

>> SCS-C03 Valid Study Materials <<

Certification SCS-C03 Questions, Updated SCS-C03 Demo

our SCS-C03 exam prep is renowned for free renewal in the whole year. As you have experienced various kinds of exams, you must have realized that renewal is invaluable to study materials, especially to such important SCS-C03 exams. And there is no doubt that being acquainted with the latest trend of exams will, to a considerable extent, act as a driving force for you to pass the SCS-C03 Exams and realize your dream of living a totally different life.

Amazon AWS Certified Security - Specialty Sample Questions (Q99-Q104):

NEW QUESTION # 99

A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.

The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.

After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.

What should the security engineer do to isolate the target instance?

- A. Create a network ACL that is associated with the target instance's subnet. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.
- B. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound

traffic. Run the document on the target instance.

- C. Remove the port 22 security group rule. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.
- D. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all ports. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all ports. Then immediately delete these rules.

Answer: A

Explanation:

Amazon EC2 security groups are stateful, meaning that once a connection is established, return traffic is automatically allowed, even if the inbound rule that originally permitted the connection is later removed.

According to the AWS Certified Security - Specialty Official Study Guide and Amazon EC2 security documentation, existing connections are not terminated when security group rules change. This explains why the SSH session remains active even after the security group rules were modified, while new traffic such as ICMP ping is blocked.

To immediately and fully isolate an EC2 instance during an incident response scenario, AWS recommends using stateless network controls. Amazon VPC network ACLs (NACLs) are stateless, which means that every packet is evaluated against the ACL rules regardless of whether the traffic is part of an existing connection.

When a deny rule is added, all traffic is immediately blocked, including active sessions.

By creating a network ACL and associating it with the subnet that contains the target instance, and by adding explicit deny rules with the lowest rule numbers for both inbound and outbound traffic, the security engineer ensures that all network communication to and from the instance is immediately interrupted. This approach satisfies the requirement to isolate the instance while preserving its runtime state and memory for forensic analysis.

Other options fail to meet the requirement because security group modifications do not terminate existing sessions, Systems Manager does not enforce network isolation, and host-level firewall changes require instance-level access and do not provide immediate, network-enforced isolation.

* AWS Certified Security - Specialty Official Study Guide

* Amazon EC2 Security Groups Documentation

* Amazon VPC Network ACL Documentation

* AWS Incident Response Best Practices

NEW QUESTION # 100

A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets. Which solution will meet these requirements?

- A. Enable AWS Config. Create a proactive AWS Config Custom Policy rule. Create a Guard clause to evaluate the S3 bucket policies to check for a value of True for the `aws:SecureTransport` condition key. If the AWS Config rule evaluates to `NON_COMPLIANT`, block resource creation.
- B. Create an AWS CloudTrail trail. Enable S3 data events on the trail. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the `aws:SecureTransport` condition key is False. Configure the CloudTrail trail to invoke the Lambda function.
- **C. Enable AWS Config. Configure the `s3-bucket-ssl-requests-only` AWS Config managed rule and set the rule trigger type to Hybrid. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the `aws:SecureTransport` condition key is False. Configure automatic remediation. Set the runbook as the target of the rule.**
- D. Enable Amazon Inspector. Create a custom AWS Lambda rule. Create a Lambda function that applies a bucket policy to deny requests when the value of the `aws:SecureTransport` condition key is False. Set the Lambda function as the target of the rule.

Answer: C

Explanation:

To enforce encryption in transit for Amazon S3, AWS best practice is to require HTTPS (TLS) by using a bucket policy condition that denies any request where `aws:SecureTransport` is false. The requirement includes both existing buckets and future buckets, so the control must continuously evaluate configuration drift and automatically remediate. AWS Config is the service intended for continuous configuration compliance monitoring across resources, and AWS Config managed rules provide standardized checks with low operational overhead. The `s3-bucket-ssl-requests-only` managed rule evaluates whether S3 buckets enforce SSL-only requests, aligning directly with enforcing encryption in transit. Setting the trigger type to Hybrid ensures evaluation both on configuration changes and periodically. Automatic remediation with an AWS Systems Manager Automation runbook allows the organization to apply or correct the bucket policy consistently at scale without manual work. This approach also supports governance by maintaining a measurable compliance status while actively fixing noncompliance. Option A is not the best fit because a "proactive" custom policy rule does not by itself remediate existing buckets and "block resource creation" is not how AWS Config

enforces controls. Option C is incorrect because Amazon Inspector is a vulnerability management service and does not govern S3 bucket transport policies. Option D is inefficient and indirect because CloudTrail data events are not a compliance engine and would require custom processing.

NEW QUESTION # 101

A company is developing an application that runs across a combination of Amazon EC2 On-Demand Instances and Spot Instances. A security engineer needs to provide a logging solution that makes logs for all instances available from a single location. The solution must allow only a specific set of users to analyze the logs for event patterns. The users must be able to use SQL queries on the logs to perform root cause analysis. Which solution will meet these requirements?

- A. Configure the EC2 instances to send application logs to a single Amazon CloudWatch Logs log group. Allow only specific users to access the log group. Use CloudWatch Logs Insights to query the log group.
- B. Configure each EC2 instance to send its application logs to its own specific Amazon CloudWatch Logs log group. Allow only specific users to access the log groups. Use Amazon Athena to query all the log groups.
- C. Configure the EC2 instances to send application logs to a single Amazon S3 bucket. Allow only specific users to access the S3 bucket. Use Amazon CloudWatch Logs Insights to query the log files in the S3 bucket.
- D. Configure the EC2 instances to send application logs to a single Amazon CloudWatch Logs log group. Grant Amazon Detective access to the log group. Allow only specific users to use Detective to analyze the logs.

Answer: A

Explanation:

Amazon CloudWatch Logs provides a centralized, scalable service for collecting and storing logs from Amazon EC2 instances, regardless of whether the instances are On-Demand or Spot Instances. According to the AWS Certified Security - Specialty Official Study Guide, CloudWatch Logs is the recommended service for centralized log aggregation and near-real-time analysis of application and system logs.

By configuring all EC2 instances to send logs to a single CloudWatch Logs log group, the security engineer ensures that logs from all instances are available in one centralized location. Access to the log group can be restricted by using IAM policies, ensuring that only authorized users can view and analyze the logs.

CloudWatch Logs Insights provides a powerful query language with SQL-like syntax, enabling users to search, filter, aggregate, and analyze log data efficiently. This directly satisfies the requirement for SQL-style queries to identify event patterns and perform root cause analysis without requiring data movement or additional services.

NEW QUESTION # 102

A company runs an online game on AWS. When players sign up for the game, their username and password credentials are stored in an Amazon Aurora database.

The number of users has grown to hundreds of thousands of players. The number of requests for password resets and login assistance has become a burden for the company's customer service team.

The company needs to implement a solution to give players another way to log in to the game.

The solution must remove the burden of password resets and login assistance while securely protecting each player's credentials. Which solution will meet these requirements?

- A. Issue API keys to new and existing players and use Amazon API Gateway for authentication.
- B. Configure Amazon Cognito user pools to federate access to the game with third-party identity providers (IdPs), such as social IdPs. Migrate the game's authentication mechanism to Cognito.
- C. When a new player signs up, use an AWS Lambda function to automatically create an IAM access key and a secret access key.
- D. Migrate the player credentials from the Aurora database to AWS Secrets Manager.

Answer: B

Explanation:

Amazon Cognito is a fully managed identity service that provides user authentication, authorization, and user management for web and mobile applications. According to AWS Certified Security - Specialty documentation, Cognito user pools are specifically designed to offload authentication responsibilities from applications while maintaining strong security controls.

By federating authentication with third-party identity providers (such as social IdPs), Cognito eliminates the need for the company to manage user passwords directly. This dramatically reduces password reset requests and customer service overhead, while also improving security through industry-standard authentication mechanisms, including MFA and token-based access.

NEW QUESTION # 103

A company runs workloads that are spread across hundreds of Amazon EC2 instances. During a recent security incident, an EC2 instance was compromised and ran malware code until the company manually terminated the instance.

The company is now using Amazon GuardDuty to detect malware on EC2 instances. A security engineer needs to implement a solution that automates a response when GuardDuty determines that an instance is infected. The solution must mitigate the incident and must comply with the AWS Well-Architected Framework guidance for incident response.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to delete all elastic network interfaces that are associated with the instance. Program the Lambda function to also add a tag of "Infected" to the instance.
- **B. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to detach all Amazon Elastic Block Store (Amazon EBS) volumes from the instance. Program the Lambda function to also add a tag of "Infected" to the EBS volumes and to terminate the instance afterward.**
- C. Define a separate VPC to isolate EC2 instances. Define a security group that does not allow any network traffic. Create an AWS Lambda function that runs when a GuardDuty scan determines that an instance is infected. Program the Lambda function to move the instance into the separate VPC and to assign the security group to the instance.
- D. Configure AWS Systems Manager Run Command to run when a GuardDuty scan determines that an instance is infected. Use Run Command to remove all network adapters from the operating system of the infected instance. Use Run Command to also add a tag of "Infected" to the instance.

Answer: B

NEW QUESTION # 104

.....

Download Amazon SCS-C03 Real Exam Dumps Today. Today is the right time to learn new and in demands skills. You can do this easily, just get registered in Amazon SCS-C03 certification exam and start preparation with Amazon SCS-C03 exam dumps. The AWS Certified Security - Specialty SCS-C03 PDF Questions and practice test are ready for download. Just pay the affordable SCS-C03 authentic dumps charges and click on the download button. Get the AWS Certified Security - Specialty SCS-C03 latest dumps and start preparing today.

Certification SCS-C03 Questions: <https://www.testkingfree.com/Amazon/SCS-C03-practice-exam-dumps.html>

Amazon SCS-C03 Valid Study Materials Finding original and latest 121 exam questions however, is a difficult process, Amazon SCS-C03 Valid Study Materials There is an old saying; nothing in the world is difficult for one who set his mind to it, When college graduates and on-job office workers in IT field learn that receiving SCS-C03 exam certification will give them an upper hand in the job market, or other benefits like promotion, many of them will decide to take part in SCS-C03 exam, Amazon SCS-C03 Valid Study Materials Fourthly, we are a company of good reputation.

You have recently been assigned to provide an accurate project schedule for a SCS-C03 troubled data conversion project, I assign a lab problem to the class, Finding original and latest 121 exam questions however, is a difficult process.

High-quality AWS Certified Security - Specialty valid exam cram & Amazon SCS-C03 dumps torrent

There is an old saying; nothing in the world is difficult Certification SCS-C03 Questions for one who set his mind to it, When college graduates and on-job office workers in IT field learn that receiving SCS-C03 Exam Certification will give them an upper hand in the job market, or other benefits like promotion, many of them will decide to take part in SCS-C03 exam.

Fourthly, we are a company of good reputation, Once you bought our SCS-C03 exam pdf, you can practice questions and study materials immediately.

- Amazon SCS-C03 Questions Latest SCS-C03 Dumps PDF [2026] Download SCS-C03 for free by simply entering [www.troytecdumps.com] website Exam SCS-C03 Materials
- Exam SCS-C03 Materials Exam SCS-C03 Certification Cost Pass SCS-C03 Guaranteed Immediately open www.pdfvce.com and search for SCS-C03 to obtain a free download New Braindumps SCS-C03 Book
- High-quality SCS-C03 Valid Study Materials Help You to Get Acquainted with Real SCS-C03 Exam Simulation Open

