Mock SCS-C03 Exams | Test SCS-C03 Result

Once you ensure your grasp on the SCS-C03 questions and answers, evaluate your learning solving the SCS-C03 practice tests provided by our testing engine. This innovative facility provides you a number of practice questions and answers and highlights the weak points in your learning. You can improve the weak areas before taking the actual test and thus brighten your chances of passing the SCS-C03 Exam with an excellent score. Moreover, doing these practice tests will impart you knowledge of the actual SCS-C03 exam format and develop your command over it.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Security Foundations and Governance: This domain addresses foundational security practices including policies, compliance frameworks, risk management, security automation, and audit procedures for AWS environments.
Topic 2	• Identity and Access Management: This domain deals with controlling authentication and authorization through user identity management, role-based access, federation, and implementing least privilege principles.
Topic 3	• Detection: This domain covers identifying and monitoring security events, threats, and vulnerabilities in AWS through logging, monitoring, and alerting mechanisms to detect anomalies and unauthorized access.
Topic 4	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.

>> Mock SCS-C03 Exams <<

Test SCS-C03 Result & New SCS-C03 Braindumps Free

Our SCS-C03 study materials are full of useful knowledge, which can meet your requirements of improvement. Also, it just takes about twenty to thirty hours for you to do exercises of the Amazon SCS-C03 Study Guide. The learning time is short but efficient. You will elevate your ability in the shortest time with the help of our Amazon SCS-C03 preparation questions.

Amazon AWS Certified Security - Specialty Sample Questions (Q93-Q98):

NEW QUESTION # 93
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. AWS CloudTrail is enabled and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

- A. Configure the ALB to export access logs to an Amazon OpenSearch Service cluster and search for the new-user-creation.php occurrences.
- B. Configure VPC Flow Logs on the subnet where the ALB is located and stream the data to CloudWatch.Search for the new-user-creation.php occurrences in CloudWatch.
- C. Configure the web ACL to send logs to Amazon Data Firehose, which delivers the logs to an S3 bucket.Use Amazon Athena to query the logs and find the new-user-creation.php occurrences.
- D. Configure the CloudWatch agent on the ALB and send application logs to CloudWatch Logs.

Answer: C

Explanation:
AWS WAF logs capturedetailed request-level information, including source IP address, request URI, headers, and rule evaluation results. According to the AWS Certified Security - Specialty documentation, AWS WAF logging is acritical detection controlwhen application-level attacks are suspected, especially when host-based logs are unreliable or can be erased by attackers.
By configuring the AWS WAF web ACL to send logs toAmazon Data Firehose, the company ensures that all future requests are centrally captured and delivered to a durable storage service such as Amazon S3. Using Amazon Athena, the security team can query these logs to identify requests targeting specific application paths such as new-user-creation.php and extract the originating client IP addresses.
Option A is incorrect because VPC Flow Logs operate at the network layer and do not capture HTTP request paths. Option B is invalid because ALBs do not support CloudWatch agents. Option C is viable but introduces additional operational complexity and cost, making it less appropriate than the native WAF logging solution.
AWS documentation highlightsAWS WAF logging combined with Athenaas a best practice for forensic analysis and attacker identification.
* AWS Certified Security - Specialty Official Study Guide
* AWS WAF Logging Documentation
* Amazon Athena User Guide
* AWS Detection and Monitoring Best Practices

NEW QUESTION # 94
A company is running an application in the eu-west-1 Region. The application uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region. A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code. Which change should the security engineer make to the AWS KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same customer managed key as the application in eu-west-1.
- B. Allocate a new customer managed key to eu-north-1. Create an alias for eu--1. Change the application code to point to the alias for eu--1.
- C. Allocate a new customer managed key to eu-north-1 to be used by the application that is deployed in that Region.
- D. Allocate a new customer managed key to eu-north-1. Create the same alias name for both keys. Configure the application deployment to use the key alias.

Answer: D

Explanation:
AWS KMS keys are regional resources and cannot be used across Regions. According to AWS Certified Security - Specialty documentation, applications that are deployed in multiple Regions should use region-specific customer managed keys while referencing keys by alias instead of key ID.
By creating a new customer managed key in eu-north-1 and assigning it the same alias as the key in eu-west-1, the application code can continue to reference the alias without modification.
Each Region resolves the alias to the correct local key, ensuring encryption continues to function correctly.
Option A is invalid because KMS keys are regional. Option B requires application changes.
Option D introduces unsupported alias patterns.
AWS best practices recommend alias-based key references for multi-Region deployments.

NEW QUESTION # 95
A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.
Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- B. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.
- C. Create an AWS Config managed rule to detect unencrypted RDS storage. Configure a manual remediation action to invoke an AWS Lambda function. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
- D. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB clusters. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscribers. Configure the Lambda function to delete the unencrypted resource.

Answer: B

Explanation:
AWS Config provides managed rules that continuously evaluate resource configurations against compliance requirements. The AWS Certified Security - Specialty documentation highlights AWS Config managed rules as the preferred mechanism for enforcing configuration compliance at scale. The managed rule for encrypted RDS storage automatically detects DB instances and clusters that are created without encryption enabled.
By configuring automatic remediation, AWS Config can immediately invoke corrective actions without manual intervention. Integrating remediation with an Amazon SNS topic enables automated email notifications, while an AWS Lambda function can terminate the noncompliant resource. This creates a fully automated detect-alert-remediate workflow.
Option B requires manual remediation, which increases operational effort and delays enforcement. Options C and D rely on Amazon EventBridge, which evaluates events rather than configuration state and does not provide continuous compliance monitoring. AWS Config is explicitly designed for configuration compliance and governance use cases.
This solution aligns with AWS governance best practices by combining continuous monitoring, automated remediation, and centralized alerting with minimal operational overhead.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Config Managed Rules
AWS Config Automatic Remediation

NEW QUESTION # 96
A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.
The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all

inbound and outbound traffic.
Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- B. Attach a security group to the VPC interface endpoint. Allow inbound traffic on port 443 to the VPC's CIDR range.
- C. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.
- D. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- E. Create an EC2 key pair. Associate the key pair with the EC2 instance.
- F. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.

Answer: B,D,F

Explanation:
AWS Systems Manager Session Manager requires secure outbound HTTPS connectivity from the EC2 instance to Systems Manager endpoints. In a VPC without internet access, AWS Certified Security - Specialty documentation recommends using interface VPC endpoints to enable private connectivity without exposing the instance to the internet.
Creating a VPC interface endpoint for Systems Manager allows the SSM Agent to communicate securely with the Systems Manager service. The endpoint must have an attached security group that allows inbound traffic on port 443 from the VPC CIDR range. Additionally, the EC2 instance security group must allow outbound HTTPS traffic on port 443 so the agent can initiate connections.
Option C is incorrect because creating or associating key pairs enables SSH access, which can alter forensic evidence and violates forensic best practices. Option B is unnecessary because Session Manager does not require inbound rules on the EC2 instance. Option F is invalid because EC2 does not use interface endpoints for management connectivity.
This combination ensures secure, private access for forensic investigation while preserving evidence integrity and adhering to AWS incident response best practices.

NEW QUESTION # 97
A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active.
How can the company continuously monitor deployment status of the software application?

- A. Use approved AMIs rule organization-wide.
- B. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: B

Explanation:
Continuous monitoring requires an always-on compliance service that evaluates resources over time. AWS Config provides managed rules that assess configuration state and compliance continuously. AWS Certified Security - Specialty guidance highlights AWS Config for continuous compliance across accounts and regions when used with AWS Organizations. The ec2-managedinstance-applications-required managed rule evaluates whether specified software is installed on managed instances, leveraging Systems Manager inventory
/managed instance status. By enabling AWS Config organization-wide and deploying this managed rule across all accounts, the company can continuously evaluate both existing and newly launched instances for required application presence. This provides a consistent compliance dashboard and history of compliance changes. Option D can provide inventory lists, but it is not a compliance rule engine that flags noncompliance with the same governance reporting and remediation pathways. Options B and C are operational approaches but do not provide continuous compliance state across the organization.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Config Managed Rules for EC2 and SSM Managed Instances
AWS Organizations Integration with AWS Config

NEW QUESTION # 98
.....

Our AWS Certified Security - Specialty (SCS-C03) exam dumps are top-notch and designed to help students pass the AWS Certified Security - Specialty (SCS-C03) test on the first try. Prep4pass offers three formats of preparation material for the SCS-C03 exam: Amazon SCS-C03 Pdf Dumps format, desktop-based SCS-C03 practice exam software, and web-based AWS Certified Security - Specialty (SCS-C03) practice test. These SCS-C03 exam dumps formats are designed to suit the needs of different types of students.

Test SCS-C03 Result: https://www.prep4pass.com/SCS-C03_exam-braindumps.html

- New SCS-C03 Dumps Free □ Pass4sure SCS-C03 Exam Prep □ SCS-C03 Vce Exam □ Enter □ www.prepawaypdf.com □ and search for ➽ SCS-C03 □ to download for free ✡ Study SCS-C03 Demo
- SCS-C03 Valid Test Pdf □ New SCS-C03 Exam Name □ SCS-C03 Test Labs □ Search for ➥ SCS-C03 □ and download it for free immediately on □ www.pdfvce.com □ □SCS-C03 Vce Exam
- Amazon SCS-C03 Exam Questions: Attain Your Professional Career Goals [2026] □ □ www.verifieddumps.com □ is best website to obtain □ SCS-C03 □ for free download □SCS-C03 Vce Exam
- Real SCS-C03 Exam Answers □ Pass4sure SCS-C03 Exam Prep □ SCS-C03 Valid Test Pdf □ Search for □ SCS-C03 □ on 「 www.pdfvce.com 」 immediately to obtain a free download □Real SCS-C03 Exam Answers
- New SCS-C03 Exam Name ↕ SCS-C03 Free Sample □ Study SCS-C03 Demo □ Go to website { www.exam4labs.com } open and search for ▹ SCS-C03 ◃ to download for free □SCS-C03 Test Labs
- SCS-C03 Free Sample □ Study SCS-C03 Demo □ SCS-C03 Test Labs □ Open website ▹ www.pdfvce.com ◃ and search for （ SCS-C03 ） for free download □New SCS-C03 Exam Name
- SCS-C03 Free Sample □ Dumps SCS-C03 Free Download □ Valid SCS-C03 Exam Format □ Simply search for ⇛ SCS-C03 ⇚ for free download on 《 www.prepawayexam.com 》 □New SCS-C03 Dumps Ebook
- Pdfvce Offer The Amazon SCS-C03 Exam Questions In Three Versions □ ☀ www.pdfvce.com □☀□ is best website to obtain 《 SCS-C03 》 for free download □SCS-C03 Vce Test Simulator
- Actual SCS-C03 Test Answers □ SCS-C03 Vce Test Simulator □ SCS-C03 Free Sample □ Go to website □ www.troytecdumps.com □ open and search for " SCS-C03 " to download for free ✉New SCS-C03 Dumps Free
- Authoritative Mock SCS-C03 Exams - Newest Source of SCS-C03 Exam □ Search for 【 SCS-C03 】 and easily obtain a free download on 《 www.pdfvce.com 》 □Actual SCS-C03 Test Answers
- Real SCS-C03 Exam Answers □ Valid SCS-C03 Exam Format □ Valid SCS-C03 Exam Format □ Open website □ www.vceengine.com □ and search for ▸ SCS-C03 ◂ for free download □SCS-C03 Valid Exam Objectives
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, learning.benindonesia.co.id, dynamictechworld.in, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, cobe2go.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes