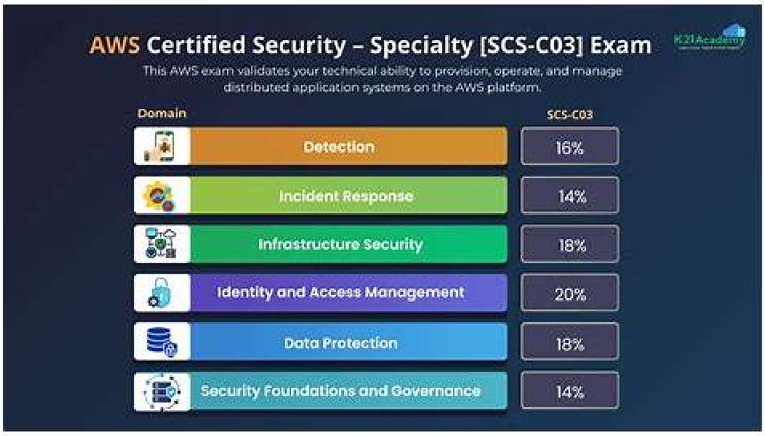
SCS-C03 Reliable Exam Price & SCS-C03 Exam Guide



AWS Certified Security – Specialty [SCS-C03] Exam

This AWS exam validates your technical ability to provision, operate, and manage distributed application systems on the AWS platform.

Domain	SCS-C03
Detection	16%
Incident Response	14%
Infrastructure Security	18%
Identity and Access Management	20%
Data Protection	18%
Security Foundations and Governance	14%

When you first contacted us with SCS-C03 quiz torrent, you may be confused about our SCS-C03 exam question and would like to learn more about our products to confirm our claims. We have a trial version for you to experience. If you encounter any questions about our SCS-C03 Learning Materials during use, you can contact our staff and we will be happy to serve for you. As for any of your suggestions, we will take it into consideration, and effectively improve our SCS-C03 exam question to better meet the needs of clients.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.
Topic 3	• 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 4	• 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 5	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.

>> SCS-C03 Reliable Exam Price <<

Amazon SCS-C03 Exam Guide | Latest SCS-C03 Test Pdf

We all know, the IT industry is a new industry, and it is one of the chains promoting economic development, so its important role can not be ignored. Our ExamsLabs's SCS-C03 exam training materials is the achievement of ExamsLabs's experienced IT experts with constant exploration, practice and research for many years. Its authority is undeniable. If you buy our SCS-C03 VCE Dumps, we will provide one year free renewal service.

Amazon AWS Certified Security - Specialty Sample Questions (Q33-Q38):

NEW QUESTION # 33

A company's security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service (Amazon SQS) queue. All the company's accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools that are outside of AWS.
What should the security engineer do to meet these requirements?

- A. Create security groups that only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the security groups to all the SQS queues in all the VPCs in the organization.
- B. In all the VPCs in the organization, adjust the network ACLs to only accept inbound traffic from the CIDR blocks of all the VPCs in the organization. Attach the network ACLs to all the subnets in all the VPCs in the organization.
- C. Use a cloud access security broker (CASB) to maintain a list of managed resources. Configure the CASB to check the API and console access against that list on a web proxy.
- D. Create interface VPC endpoints for Amazon SQS in all the VPCs in the organization. Set the aws: SourceVpce condition to the VPC endpoint identifier on the SQS policy. Add the aws:PrincipalOrgId condition to the VPC endpoint policy.

Answer: D

Explanation:
Amazon SQS is an AWS-managed service and does not operate within customer VPCs. Therefore, security groups and network ACLs cannot be used to control access to SQS, making options A and B invalid.
According to AWS Certified Security - Specialty documentation, the recommended approach to securely access AWS services from within a VPC is through interface VPC endpoints (AWS PrivateLink).
By creating interface VPC endpoints for Amazon SQS, the company ensures that traffic to SQS stays within the AWS network and does not traverse the public internet. Adding an SQS resource policy with the aws:SourceVpce condition restricts access so that only requests originating from the specified VPC endpoint are allowed. Additionally, using the aws:PrincipalOrgId condition ensures that only principals belonging to the same AWS Organization can access the queue.
Option D introduces an external tool, increasing cost and compliance complexity, which directly violates the requirement to minimize investment outside AWS.
AWS documentation clearly identifies VPC endpoints combined with IAM condition keys as a best practice for securing service access in multi-account environments.
* AWS Certified Security - Specialty Official Study Guide
* Amazon SQS Security Best Practices
* AWS Organizations Documentation
* AWS PrivateLink User Guide

NEW QUESTION # 34
A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet.
The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC.
Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

- A. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.
- B. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
- C. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
- D. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
- E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.

Answer: D,E

Explanation:
AWS networking best practices require private subnets to access the internet only through NAT gateways located in public subnets.
According to the AWS Certified Security - Specialty Study Guide, NAT gateways must be provisioned in public subnets and used as the default route for outbound traffic from private subnets.
Verifying NAT gateways in each Availability Zone ensures high availability and fault tolerance. Updating the private subnet route tables to send 0.0.0.0/0 traffic to the NAT gateway prevents direct internet access while allowing outbound connectivity.
Routing private subnet traffic directly to an internet gateway violates subnet isolation principles. NAT gateways must never be placed in private subnets.

Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon VPC Routing and NAT Gateways
AWS Network Segmentation Best Practices

NEW QUESTION # 35

A security engineer is working with a development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS Key Management Service (AWS KMS) customer managed key to encrypt the data in Amazon S3.

The inventory data in Amazon S3 will be shared with hundreds of vendors. All vendors will use AWS principals from their own AWS accounts to access the data in Amazon S3. The vendor list might change weekly. The security engineer needs to find a solution that supports cross-account access.

Which solution is the MOST operationally efficient way to manage access control for the customer managed key?

- A. Use am IAM role to manage key access. Programmatically update the IAM role policies to manage vendor access.
- B. Use delegated access across AWS accounts by using IAM roles to manage key access.Programmatically update the IAM trust policy to manage cross-account vendor access.
- C. Use KMS key policies to manage key access. Programmatically update the KMS key policies to manage vendor access.
- D. Use KMS grants to manage key access. Programmatically create and revoke grants to manage vendor access.

Answer: D

Explanation:

KMS grants provide a scalable and efficient way to manage access to AWS KMS customer- managed keys, especially for cross-account access. Grants allow you to specify who can use the key and what operations they can perform on it without needing to modify the KMS key policy itself. Grants are flexible and can be created, modified, and revoked programmatically, making them ideal for situations where the vendor list changes frequently.

This approach minimizes operational overhead while allowing the security engineer to dynamically control access to the KMS key as vendor requirements change.

NEW QUESTION # 36

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 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.
- C. 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.
- 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: C

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 # 37

A company has a large fleet of Amazon Linux 2 Amazon EC2 instances that run an application. The application processes sensitive data and has the following compliance requirements:
* No remote access management ports to the EC2 instances can be exposed internally or externally.
* All remote session activity must be recorded in an audit log.
* All remote access to the EC2 instances must be authenticated and authorized by AWS IAM Identity Center.
The company's DevOps team occasionally needs to connect to one of the EC2 instances to troubleshoot issues.
Which solution will provide remote access to the EC2 instances while meeting the compliance requirements?

- A. Assign an EC2 instance role that allows access to AWS Systems Manager. Create an IAM policy that grants access to Systems Manager Session Manager. Assign the policy to an IAM role of the DevOps team.
- B. Grant access to the EC2 serial console at the account level.
- C. Enable EC2 Instance Connect and configure security group rules.
- D. Use AWS Systems Manager Automation runbooks to open remote access ports.

Answer: A

Explanation:
AWS Systems Manager Session Manager providessecure, auditable, and portless accessto EC2 instances.
According to the AWS Certified Security - Specialty Study Guide, Session Manager allows administrators to connect to instanceswithout opening inbound SSH or RDP ports, fully satisfying strict compliance requirements.
Session Manager integrates directly withAWS IAM Identity Center, ensuring that all access is authenticated and authorized using centralized identity management. Additionally, Session Manager automatically records session activity and can send logs to Amazon CloudWatch Logs or Amazon S3, providing a complete audit trail of all commands executed during a session.
Option A (EC2 serial console) does not provide comprehensive auditing and is intended for recovery scenarios. Option B requires inbound network access and security group rules, violating the "no exposed management ports" requirement. Option D explicitly opens ports, which directly violates compliance constraints.
AWS documentation clearly identifiesSystems Manager Session Manager as the recommended solution for secure, auditable, and identity-integrated instance accessin regulated environments.
* AWS Certified Security - Specialty Official Study Guide
* AWS Systems Manager Session Manager Documentation
* AWS IAM Identity Center Best Practices

NEW QUESTION # 38

......

About the SCS-C03 Exam Certification, reliability can not be ignored. SCS-C03 exam training materials of ExamsLabs are specially designed. It can maximize the efficiency of your work. We are the best worldwide materials provider about this exam.

SCS-C03 Exam Guide: https://www.examslabs.com/Amazon/AWS-Certified-Specialty/best-SCS-C03-exam-dumps.html

- Amazon SCS-C03 dumps - Testinsides SCS-C03 PDF - SCS-C03 actual test □ Search for ➡ SCS-C03 □□□ and download it for free on □ www.pdfvce.com □ website □SCS-C03 Latest Study Materials
- SCS-C03 Certification Exam Dumps □ SCS-C03 Reliable Test Experience □ SCS-C03 Certification Exam Dumps □ Search on 《 www.prepawaypdf.com 》 for （ SCS-C03 ） to obtain exam materials for free download □Valid SCS-C03 Vce
- Latest Amazon SCS-C03 Exam Questions in Three Different Formats □ Search for ➠ SCS-C03 □ and download it for free on □ www.pdfvce.com □ website □SCS-C03 Dumps Discount
- SCS-C03 Dumps Discount □ Certification SCS-C03 Book Torrent □ Original SCS-C03 Questions □ Open （ www.prepawaypdf.com ） and search for ☀ SCS-C03 □☀□ to download exam materials for free □Valid SCS-C03 Test Cram
- Amazon SCS-C03 Reliable Exam Price: AWS Certified Security - Specialty - Pdfvce 10 Years of Excellence □ Search for ✔ SCS-C03 □✔□ and download it for free immediately on ➤ www.pdfvce.com □ □SCS-C03 Dumps Discount
- Free PDF Reliable SCS-C03 - AWS Certified Security - Specialty Reliable Exam Price □ Enter ➥ www.dumpsmaterials.com □ and search for 【 SCS-C03 】 to download for free □Frequent SCS-C03 Updates
- Amazon SCS-C03 Reliable Exam Price: AWS Certified Security - Specialty - Pdfvce 10 Years of Excellence □ Simply search for 「 SCS-C03 」 for free download on ➥ www.pdfvce.com □ ♻Frequent SCS-C03 Updates
- SCS-C03 Valid Test Testking □ SCS-C03 Latest Study Materials □ Latest SCS-C03 Test Preparation □ Enter ➠ www.examdiscuss.com □ and search for 「 SCS-C03 」 to download for free □Latest SCS-C03 Test Preparation
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes