Test SCS-C03 Lab Questions & SCS-C03 Testking Exam Questions

It-Tests provides Amazon SCS-C03 exam questions for the SCS-C03 exam in PDF format. The SCS-C03 exam questions pdf file is easy to understand and can be downloaded on all smart devices. You can access your SCS-C03 practice exam questions pdf by downloading the SCS-C03 Exam Questions on your PC, laptop, Mac, tablet, and smartphone. You can use the SCS-C03 pdf questions at any time and anywhere you want, making exam preparation convenient and accessible from the comfort of your home.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• Incident Response: This domain addresses responding to security incidents through automated and manual strategies, containment, forensic analysis, and recovery procedures to minimize impact and restore operations.

>> Test SCS-C03 Lab Questions <<

SCS-C03 Testking Exam Questions & SCS-C03 Latest Material

About the oncoming SCS-C03 exam, every exam candidates are wishing to utilize all intellectual and technical skills to solve the obstacles ahead of them to go as well as it possibly could. So the pending exam causes a panic among the exam candidates. The SCS-C03 exam prepare of our website is completed by experts who has a good understanding of real exams and have many years of experience writing SCS-C03 Study Materials. They know very well what candidates really need most when they prepare for the exam. They also understand the real exam situation very well. So they compiled SCS-C03 exam prepare that they hope to do their utmost to help candidates pass the exam and get what job they want.

Amazon AWS Certified Security - Specialty Sample Questions (Q43-Q48):

NEW QUESTION # 43
A corporate cloud security policy states that communications 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. Create a VPC endpoint for AWS KMS withprivate DNS enabled.
- 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. Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
- D. Add theaws:sourceVpcecondition to the AWS KMS key policy referencing the company ' s VPC endpoint ID.
- E. Add the following condition to the AWS KMS key policy: " aws:SourceIp " : " 10.0.0.0/16 " .

Answer: A,D

Explanation:
To ensure traffic from a VPC to AWS KMS stays on the AWS network and does not use public endpoints, you should use aninterface VPC endpoint (AWS PrivateLink) for KMS. Creating aVPC endpoint for KMS with private DNS enabled(Option C) causes standard KMS DNS names (for example, kms. < region > .
amazonaws.com) to resolve to theprivateendpoint IPs inside the VPC, routing requests over the AWS private network rather than through the internet. This is the core networking control that satisfies "no public service endpoints." To enforce that only calls that come through the intended VPC endpoint can use the key, add an authorization guardrail in theKMS key policyusing the aws:sourceVpce condition (Option A). This ensures that even if a principal has credentials, KMS will deny usage unless the request is made via the specified VPC endpoint, preventing accidental or malicious use over public paths.
Option B is neither necessary nor sufficient: removing an internet gateway does not prevent all public endpoint use (NAT, other egress paths, or other VPCs could still be involved) and can break workloads.
Option D is unrelated to runtime KMS API traffic. Option E is weaker because SourceIp checks can be bypassed via other AWS network paths and does not guarantee PrivateLink usage the way sourceVpce does.

NEW QUESTION # 44
A company needs a cloud-based, managed desktop solution for its workforce of remote employees. The company wants to ensure that the employees can access the desktops only by using company-provided devices. A security engineer must design a solution that will minimize cost and management overhead.
Which solution will meet these requirements?

- A. Deploy a fleet of Amazon EC2 instances. Assign an instance to each employee with certificate-based device authentication that uses Windows Active Directory.
- B. Deploy Amazon WorkSpaces. Set up a trusted device policy with IP blocking on the authentication gateway by using AWS Identity and Access Management (IAM).
- C. Deploy a custom virtual desktop infrastructure (VDI) solution with a restriction policy to allow access only from corporate devices.
- D. Deploy Amazon WorkSpaces. Create client certificates, and deploy them to trusted devices. Enable restricted access at the directory level.

Answer: D

Explanation:
Amazon WorkSpaces is a fully managed desktop-as-a-service solution designed to minimize infrastructure and operational overhead. According to AWS Certified Security - Specialty documentation, WorkSpaces supports device trust by using client certificates to restrict access to approved devices.
By deploying client certificates only to company-managed devices and enforcing restricted access at the directory level, the organization ensures that only trusted endpoints can authenticate. This approach avoids the cost and complexity of building and maintaining a custom VDI or managing individual EC2 instances.
Option A and B significantly increase management overhead. Option C is incorrect because IAM does not manage WorkSpaces authentication gateway policies or device trust.
AWS best practices highlight Amazon WorkSpaces with certificate-based device trust as the most efficient solution for secure, managed desktops.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon WorkSpaces Security Controls
Amazon WorkSpaces Device Trust

NEW QUESTION # 45
A company needs to detect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The solution must require no additional configuration of the existing EKS deployment.

Which solution will meet these requirements with the LEAST operational effort?

- A. Enable AWS Security Hub and monitor Kubernetes findings.
- B. Install a third-party security add-on.
- C. Monitor CloudWatch Container Insights metrics for EKS.
- D. Enable Amazon GuardDuty and use EKS Audit Log Monitoring.

Answer: D

Explanation:
Amazon GuardDuty provides managed threat detection and supports EKS protection features that analyze Kubernetes audit logs to detect suspicious activity, including unauthorized or unauthenticated access attempts.
AWS Certified Security - Specialty documentation recommends GuardDuty for low-overhead detection because it is fully managed and does not require deploying agents or modifying application code. EKS Audit Log Monitoring is designed to consume and analyze relevant control plane audit events to identify anomalous or unauthorized actions against the cluster. Compared to third-party add-ons, GuardDuty reduces operational burden and remains fully within AWS managed services. Security Hub aggregates findings from services like GuardDuty but does not itself perform the detection. CloudWatch Container Insights focuses on performance and operational metrics, not authentication security detections. Therefore, enabling GuardDuty with EKS Audit Log Monitoring provides the required detection with the least operational effort and without requiring additional configuration to the existing EKS workload beyond enabling the feature.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon GuardDuty EKS Protection and Audit Log Monitoring
AWS Threat Detection Best Practices for Kubernetes on AWS

NEW QUESTION # 46
A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible. Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Enable AWS Security Hub in the AWS account.
- B. Create an Amazon EventBridge rule for GuardDuty findings of high severity. Configure the rule to publish a message to the topic.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email distribution list to the queue.
- D. Create an Amazon EventBridge rule for Security Hub findings of high severity. Configure the rule to publish a message to the queue.
- E. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email distribution list to the topic.
- F. Enable Amazon GuardDuty in the AWS account.

Answer: B,E,F

Explanation:
Amazon GuardDuty provides continuous threat detection for compromised instances by analyzing VPC Flow Logs, DNS logs, and CloudTrail events. According to AWS Certified Security - Specialty guidance, GuardDuty is the fastest service to enable for detecting malware and compromised EC2 instances.
To notify the security team, Amazon SNS provides a native email notification mechanism with minimal setup. Amazon EventBridge integrates directly with GuardDuty findings and can filter based on severity. Creating an EventBridge rule that matches high severity GuardDuty findings and publishes to SNS ensures immediate notification.
Security Hub is not required for this use case and adds additional setup time. Amazon SQS does not support email subscriptions.

NEW QUESTION # 47
A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to

access the company's AWS resources.
Which additional step will meet these requirements?

- A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
- B. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permissions. Use the credentials to generate the pre-signed URLs.
- C. Add a StringEquals condition to the IAM role policy for the EC2 instance profile. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoice. Tag each generated invoice with the ID of its corresponding client.
- D. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucket. Embed the keys into the script. Use the keys to generate the pre-signed URLs.

Answer: C

Explanation:
Amazon S3 pre-signed URLs grant temporary access based on the permissions of the principal that generates them. AWS Certified Security - Specialty documentation explains that fine-grained authorization can be enforced by combining pre-signed URLs with IAM policy conditions.
By tagging each invoice object with a client identifier and adding a condition to the EC2 instance role policy using s3:ResourceTag/ClientId, the role can generate pre-signed URLs only for objects associated with a specific client. This ensures that each client can access only their own invoices, even though the URLs are temporary and unauthenticated.
Option A over-permissions clients. Option C is unnecessary because instance profiles already use temporary credentials. Option D violates AWS best practices by using long-term credentials.
AWS recommends resource tagging with IAM policy conditions for scalable, secure access control.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon S3 Pre-Signed URLs
IAM Policy Conditions and Resource Tags

NEW QUESTION # 48
.....

- Authoritative Test SCS-C03 Lab Questions - Newest Source of SCS-C03 Exam □ Go to website [www.pdfvce.com] open and search for 《 SCS-C03 》 to download for free □SCS-C03 Reliable Test Topics
- Valid SCS-C03 Mock Exam □ New SCS-C03 Exam Testking □ Latest SCS-C03 Dumps Ppt □ Open website ☀ www.practicevce.com □☀□ and search for ➽ SCS-C03 □ for free download □Reliable SCS-C03 Test Cost
- 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, www.stes.tyc.edu.tw, teacherrahmat.com, 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, 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.askmap.net, 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, shufaii.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes