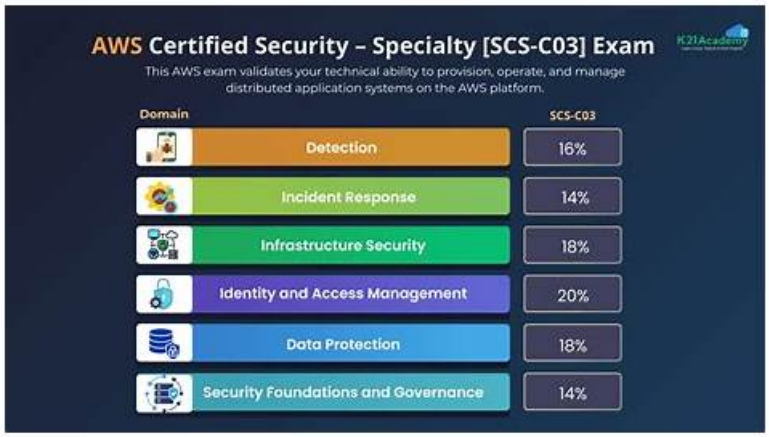
Reliable SCS-C03 Braindumps Pdf, Sure SCS-C03 Pass



P.S. Free & New SCS-C03 dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1MZUaT5pLZynrwmmC0SW9WmeFdNhpV-ok

As you can find on our website, our SCS-C03 practice questions have three versions: the PDF, Software and APP online. If you want to study with computers, our online test engine and the windows software of the SCS-C03 exam materials will greatly motivate your spirits. The exercises can be finished on computers, which can help you get rid of the boring books. The operation of the SCS-C03 Study Guide is extremely smooth because the system we design has strong compatibility with your computers.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.
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	• 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.

>> Reliable SCS-C03 Braindumps Pdf <<

Sure SCS-C03 Pass - Valid SCS-C03 Real Test

Real4test is aware of your busy routine; therefore, it has made the AWS Certified Security - Specialty SCS-C03 dumps format to facilitate you to prepare for the AWS Certified Security - Specialty SCS-C03 exam. We adhere strictly to the syllabus set by Amazon SCS-C03 Certification Exam. What will make your SCS-C03 test preparation easy is its compatibility with all devices such as PCs, tablets, laptops, and androids.

Amazon AWS Certified Security - Specialty Sample Questions (Q154-Q159):

NEW QUESTION # 154
A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances.

Which solution will meet these requirements?

- A. Install EC2 Instance Connect on the EC2 instances. Update the IAM policy for the IAM role to grant the required permissions. Use the AWS CLI to open a tunnel to connect to the instances.
- B. Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS Management Console to connect to the EC2 instances.
- C. Install EC2 Instance Connect on the EC2 instances. Configure the instances to permit access to the ec2- instance-connect command user. Use the AWS Management Console to connect to the EC2 instances.
- D. Create an EC2 Instance Connect endpoint in the VPC. Configure an appropriate security group to allow access between the EC2 instances and the endpoint. Use the AWS CLI to open a tunnel to connect to the instances.

Answer: B

Explanation:
During an incident, the company wants to block "external access to the VPC" (for example, shutting down VPN ingress or internet-exposed paths) yet still allow the security team to access instances for forensics.
AnEC2 Instance Connect Endpoint (EIC Endpoint)provides a managed, private connectivity path that lets authorized users connect to instances in a VPCwithout requiring inbound access from the internet or from on- premises. The endpoint lives inside the VPC, and access is controlled by IAM permissions plus security group rules between the endpoint and the instances. This supports incident containment (no external network entry) while preserving controlled administrative access for investigation.
Options A and B require installing Instance Connect on the instances and typically rely on network reachability patterns that may be blocked when external access is cut off; they also do not provide the same VPC-resident endpoint model. With an EIC endpoint, the security team can use theAWS Management Consoleto initiate connections (Option D) even while the VPC is isolated from on-prem and the public internet, because the connectivity is mediated through AWS control plane and the endpoint inside the VPC.
Option C mentions using the CLI to open a tunnel, but the most straightforward and commonly used operational method for responders is console-based access via the EIC endpoint. Therefore, creating an Instance Connect Endpoint and using the console meets the requirement.

NEW QUESTION # 155
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 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.
- B. 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.
- 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. 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.

Answer: A

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.

NEW QUESTION # 156
A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications.
The leader of the company's application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.
The team members access the account by assuming a role that has a specific set of permissions. All team members have permissions to perform operations on the stacks.
Which combination of steps will ensure consistent deployment of the stacksMOST securely? (Select THREE.)

- A. Add policies that reference each CloudFormation stack ARN.
- B. Add a policy to each member role to allow the iam:PassRole action for the service role.
- C. Create a service role that has cloudformation.amazonaws.com as the service principal.
- D. Update each stack to use the service role.
- E. Add policies that reference the ARNs of each AWS service that requires permissions.
- F. Create a service role that has a composite principal that contains each service that needs the necessary permissions.

Answer: B,C,D

Explanation:
AWS CloudFormation supports the use of aservice role, which allows CloudFormation to assume a dedicated IAM role to create and manage resources on behalf of users. According to the AWS Certified Security - Specialty Study Guide, using a service role is themost secure and consistent wayto ensure predictable stack deployments when users have varying permission sets.
By creating a service role with cloudformation.amazonaws.com as the trusted service principal (Option B), CloudFormation-not individual users-assumes responsibility for resource creation. Updating each stack to explicitly use this service role (Option E) ensures that all deployments use the same permission set, eliminating inconsistencies.
Granting the team members permission to pass the service role via iam:PassRole (Option F) is required so that CloudFormation can assume the role during stack operations. This approach adheres to the principle of least privilege and prevents users from gaining direct access to elevated permissions.
Composite principals (Option A) are unnecessary and insecure. Referencing stack ARNs (Option C) does not solve the root cause. While Option D reflects good policy design, it is implicit in creating the service role and is not a required standalone step.
AWS documentation clearly identifiesCloudFormation service roles combined with iam:PassRoleas best practice for secure, consistent infrastructure deployments.
* AWS Certified Security - Specialty Official Study Guide
* AWS CloudFormation Service Role Documentation
* AWS IAM Best Practices

NEW QUESTION # 157
A company uses AWS IAM Identity Center to manage access to its AWS accounts. The accounts are in an organization in AWS Organizations. A security engineer needs to set up delegated administration of IAM Identity Center in the organization's management account. Which combination of steps should the security engineer perform in IAM Identity Center before configuring delegated administration? (Select THREE.)

- A. Create permission sets for use only in the organization's management account.
- B. Grant least privilege access to the organization's management account.
- C. Create IAM users for use only in the organization's management account.
- D. Set up a second AWS Region in the organization's management account.
- E. Create a new IAM Identity Center directory in the organization's management account.
- F. Create user assignments only in the organization's management account.

Answer: A,E,F

Explanation:
AWS IAM Identity Center delegated administration requires foundational configuration to be completed in the organization's management account before delegation. According to the AWS Certified Security - Specialty documentation, IAM Identity Center must be enabled with a directory in the management account before any delegation can occur.
Permission sets must be created in the management account because they define the permissions that will later be delegated to member accounts. Additionally, user assignments must initially exist in the management account to establish baseline access control before delegation is configured.
Option A is too generic and not a required prerequisite step. Option C is unrelated to Identity Center delegation. Option E is incorrect because IAM Identity Center uses identities from its directory or external IdPs, not IAM users.
AWS guidance clearly outlines directory creation, permission set definition, and initial user assignments as mandatory preparatory

steps for delegated administration.

NEW QUESTION # 158
A company has a compliance requirement to encrypt all data in transit. The company recently discovered an Amazon Aurora cluster that does not meet this requirement.
How can the company enforce encryption for all connections to the Aurora cluster?

- A. Configure the Aurora cluster to use AWS Certificate Manager (ACM) to provide encryption certificates.
- B. In the Aurora cluster configuration, set therequire_secure_transportDB cluster parameter toON.
- C. Use AWS Directory Service for Microsoft Active Directory to create a user directory and to enforce Kerberos authentication with Aurora.
- D. Create an Amazon RDS proxy. Connect the proxy to the Aurora cluster to enable encryption.

Answer: B

Explanation:
To enforce encryption in transit to Aurora, you must require clients to useTLS/SSLwhen connecting to the database. Aurora (depending on engine flavor) supports a parameter that enforces secure transport by rejecting non-TLS connections. Setting the DB (cluster/instance) parameter such asrequire_secure_transporttoONforces clients to negotiate SSL/TLS; otherwise the server refuses the connection, ensuring all data in transit is encrypted. This directly enforces the compliance requirement at the database endpoint itself, independent of client behavior.
Kerberos authentication (Option B) provides centralized authentication and can be useful for IAM/AD integration, but it does not by itself guarantee that the network session is encrypted. Option C is incorrect because Aurora/RDS usesRDS-provided certificatesfor TLS; you don't attach ACM certificates to Aurora the way you would for ALB/CloudFront. Option D is not the right enforcement mechanism: RDS Proxy can help with connection pooling and IAM auth patterns, but it does not inherently force all client-to-proxy or proxy-to- db connections to be encrypted in the way a DB parameter enforcement does (and you'd still need to ensure clients use TLS). Therefore, enabling the parameter that requires secure transport is the correct solution.

NEW QUESTION # 159
.....

- SCS-C03 Review Guide □ SCS-C03 Review Guide □ SCS-C03 Sample Test Online □ Search on ➡ www.testkingpass.com □□□ for 《 SCS-C03 》 to obtain exam materials for free download □SCS-C03 Review Guide
- SCS-C03 Exam Bootcamp - SCS-C03 Latest Dumps - SCS-C03 Study Materials □ Go to website ➥ www.pdfvce.com □ open and search for ✔ SCS-C03 □✔□ to download for free □SCS-C03 Review Guide
- Latest SCS-C03 Exam Objectives □ SCS-C03 Review Guide □ SCS-C03 Exam Introduction □ Open website ➤ www.prep4away.com □ and search for 【 SCS-C03 】 for free download □SCS-C03 Review Guide
- graphiskill.com, www.benzou.cn, www.grepmed.com, www.stes.tyc.edu.tw, h.kongminghu.com, rasmir.com, www.stes.tyc.edu.tw, tooter.in, justpaste.me, dahannbbs.com, Disposable vapes

P.S. Free & New SCS-C03 dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1MZUaT5pLZynrwmmC0SW9WmeFdNhpV-ok