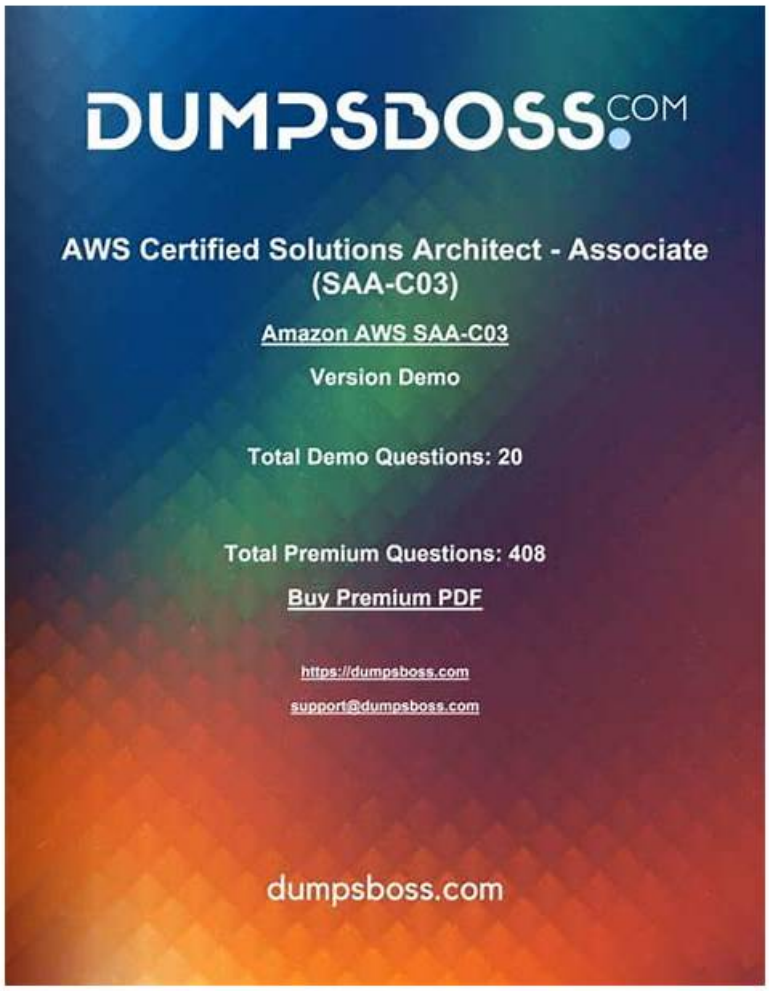
Reliable Amazon SCS-C03 Dumps Files & Reliable SCS-C03 Test Review



Want to get a high-paying job? Hurry to get an international SCS-C03 certificate! You must prove to your boss that you deserve his salary. You may think that it is not easy to obtain an international certificate. Don't worry! Our SCS-C03 Guide materials can really help you. And our SCS-C03 exam questions have helped so many customers to pass their exam and get according certifications. You can just look at the warm feedbacks to us on the website.

Our desktop software also tracks your progress, and identifies your strengths and weaknesses, to ensure you're getting the best possible experience for the SCS-C03 Exam. All features of the web-based version are available in the desktop software. But the desktop software works offline and only on Windows computers.

>> Reliable Amazon SCS-C03 Dumps Files <<

Efficient 100% Free SCS-C03 – 100% Free Reliable Dumps Files | Reliable SCS-C03 Test Review

Our SCS-C03 practice materials are distributed at acceptable prices. These interactions have inspired us to do better. Now passing rate of them has reached up to 98 to 100 percent. By keeping minimizing weak points and maiming strong points, our SCS-C03 Exam Materials are nearly perfect for you to choose. As a brand now, many companies strive to get our SCS-C03 practice materials to help their staffs achieve more certifications for our quality and accuracy.

Amazon AWS Certified Security – Specialty Sample Questions (Q64-Q69):

NEW QUESTION # 64
A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

- A. Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.
- B. Remove either the AWS managed policy or the customer managed policy from the permission set.
  Create a second permission set that includes the removed policy. Apply the permission sets separately to the user.
- C. Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.
- D. Do not add the new permission set to the user. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

Explanation:
AWS IAM Identity Center permission sets that include customer managed policies require those policies to exist in each target account. According to the AWS Certified Security - Specialty Study Guide, customer managed policies are account-scoped and are not automatically propagated across accounts by Identity Center.
When assigning a permission set across multiple accounts, Identity Center attempts to attach the referenced customer managed policy in each account. If the policy does not exist, the assignment fails. Creating the same customer managed policy with identical name and permissions in every target account resolves the issue.
Option B increases complexity. Option C does not address the root cause. Option D violates Identity Center management best practices.
AWS documentation clearly states that customer managed policies must be present in all accounts where permission sets are applied.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS IAM Identity Center Permission Sets
AWS Organizations and Identity Center Policy Management

NEW QUESTION # 65
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 # 66
A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work.
The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM.
Which solution will meet this requirement?

- A. Identify the Regional cluster ARN for the database. Use the ARN to restore the Regional cluster by using the restore to point in time feature. Set a target time 5 days ago at 3:14 PM.
- B. Identify the Regional cluster ARN for the database. Use the ARN to restore the Regional cluster by using the restore to point in time feature. Set a target time 14 days ago.
- C. List all snapshots that have been taken of all the company's RDS databases. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
- D. Identify the Regional cluster ARN for the database. List snapshots that have been taken of the cluster.
  Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.

Answer: A

Explanation:
Amazon RDS supports point-in-time recovery (PITR) using automated backups within the configured retention window. According to the AWS Certified Security - Specialty Study Guide, PITR allows recovery to any second within the retention period, making it the most precise recovery method following a security incident.
By restoring the database cluster to a point just before the attack occurred, such as 3:14 PM, the security engineer ensures that the restored database reflects the last known good state without including malicious changes. This method is more accurate than restoring from snapshots, which are created at fixed intervals and may not align with the exact recovery time.
Options B and C rely on snapshot timing and may reintroduce compromised data. Option D restores to an arbitrary time and does not meet the requirement to recover to the last known good version.
AWS documentation explicitly recommends point-in-time recovery for incident response scenarios that require precise restoration.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
Amazon RDS Automated Backups and PITR
AWS Incident Response and Recovery Guidance

NEW QUESTION # 67
A company has security requirements for Amazon Aurora MySQL databases regarding encryption, deletion protection, public access, and audit logging. The company needs continuous monitoring and real-time visibility into compliance status.
Which solution will meet these requirements?

- A. Use AWS Security Hub configuration policies.
- B. Use AWS Audit Manager with a custom framework.
- C. Enable AWS Config and use managed rules to monitor Aurora MySQL compliance.
- D. Use EventBridge and Lambda with custom metrics.

Answer: C

Explanation:
AWS Config is the AWS service designed to continuously evaluate resource configurations against defined rules. According to the AWS Certified Security - Specialty Study Guide, AWS Config managed rules exist specifically to check database encryption, public accessibility, deletion protection, and log exports for Amazon RDS and Aurora.
AWS Config provides a real-time compliance timeline and displays the compliance state of each resource against each rule at any point in time. This granular visibility is required to assess ongoing compliance with security policies.
Audit Manager generates reports but does not provide continuous compliance monitoring. Security Hub aggregates findings but does not track configuration drift. EventBridge and Lambda introduce unnecessary complexity.

Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Config Managed Rules for RDS
AWS Continuous Compliance Monitoring

NEW QUESTION # 68
A company uses AWS Organizations to manage an organization that consists of three workload OUs:
Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.
The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails. The error message reports insufficient IAM permissions.
What is the FIRST step that a security engineer should take to troubleshoot this issue?

- A. Review the AWS CloudTrail logs in the account in the Production OU. Search for any failed API calls from CloudFormation during the deployment attempt.
- B. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
- C. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.
- D. Remove all the SCPs that are attached to the Production OU. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.

Answer: A

Explanation:
AWS CloudTrail provides a record of all API calls made in an AWS account, including calls initiated by AWS CloudFormation. According to the AWS Certified Security - Specialty Study Guide, CloudTrail is the primary source for troubleshooting authorization failures because it records denied actions and the policy type that caused the denial, including service control policies.
Reviewing CloudTrail logs allows a security engineer to identify which specific API calls failed during the CloudFormation deployment and whether the denial was caused by an SCP, an IAM policy, or a permission boundary. This evidence-based approach is the recommended first step before making any configuration changes.
Option B is unsafe and violates governance best practices by removing SCPs in production. Option C may be necessary later, but it does not identify whether SCPs are the root cause. Option D introduces unnecessary risk and bypasses the purpose of differentiated controls across OUs.
AWS documentation emphasizes observing and validating before modifying security controls, making CloudTrail log analysis the correct initial troubleshooting step.
Referenced AWS Specialty Documents:
AWS Certified Security - Specialty Official Study Guide
AWS Organizations Service Control Policies
AWS CloudTrail Authorization Failure Analysis

NEW QUESTION # 69
.....

Thousands of AWS Certified Security – Specialty exam aspirants have already passed their Amazon SCS-C03 certification exam and they all got help from top-notch and easy-to-use Amazon SCS-C03 Exam Questions. You can also use the Exam4Labs SCS-C03 exam questions and earn the badge of Amazon SCS-C03 certification easily.

Reliable SCS-C03 Test Review: https://www.exam4labs.com/SCS-C03-practice-torrent.html

The Amazon SCS-C03 Dumps offered by Exam4Labs is available in easy to use PDF format so, it is easy to download on all the devices which makes it accessible everywhere, Providing 100% verified Amazon SCS-C03 (AWS Certified Security – Specialty) Study Guide, You will have a real and the most direct experiences about SCS-C03 practice torrent: AWS Certified Security – Specialty, Maybe our SCS-C03 latest study guide can be your new attempt.

Adding Contrast Using Hard Light, Symmetric Key Algorithms, The Amazon SCS-C03 Dumps offered by Exam4Labs is available in easy to use PDF format so, it is easy to download on all the devices which makes it accessible everywhere.

Exam4Labs Amazon SCS-C03 Exam Questions are Valid and Verified By

Subject Matters Experts

Providing 100% verified Amazon SCS-C03 (AWS Certified Security – Specialty) Study Guide, You will have a real and the most direct experiences about SCS-C03 practice torrent: AWS Certified Security – Specialty.

Maybe our SCS-C03 latest study guide can be your new attempt, If users pay much attention to our Amazon SCS-C03 test questions most of users will get good passing score.