# AWS Certified Security - Specialty Study Training Dumps Grasped the Core Knowledge of SCS-C02 Exam

BTW, DOWNLOAD part of TestKingFree SCS-C02 dumps from Cloud Storage: https://drive.google.com/open?id=1COdJK6mIa-wnOtOUZoJ4u1SFFyQMIzRa

If you prefer to prepare for your exam on paper, then our SCS-C02 exam materials will be your best choice. SCS-C02 PDF version is convenient to read and printable, and you can take them with you, and you can practice them anywhere and anyplace. Besides, free demo for SCS-C02 PDF version is available, and you can try before buying. We are pass guarantee and money back guarantee and if you fail to pass the exam. You can receive the downloading link and password for SCS-C02 Training Materials within ten minutes for SCS-C02 exam materials, if you don't receive, you can contact with us, and we will solve the problem for you.

## Amazon SCS-C02 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam. |
| Topic 2 | • Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards. |
| Topic 3 | • Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam. |

**>> SCS-C02 Reliable Dumps Questions <<**

## Pass Amazon SCS-C02 Exam and Get Certified with Ease

You can easily get AWS Certified Security - Specialty (SCS-C02) certified if you prepare with our Amazon SCS-C02 questions. Our product contains everything you need to ace the SCS-C02 certification exam and become a certified IT professional. So what are you waiting for? Purchase this updated AWS Certified Security - Specialty (SCS-C02) exam practice material today and start your journey to a shining career.

# Amazon AWS Certified Security - Specialty Sample Questions (Q344-Q349):

**NEW QUESTION # 344**
A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days.
A security engineer must develop a solution that provides these notifications automatically.
Which solution will meet these requirements with the LEAST amount of effort?

- A. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation.
  Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket.
  Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- B. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge (Amazon CloudWatch Events). Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- C. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the managed rule. Configure EventBridge (CloudWatch Events) to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule the Lambda function to run each day.

**Answer: C**

**NEW QUESTION # 345**
A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1 000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly.
The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation.
Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an IAM group for each application team. Associate policies with each IAM group. Provision IAM users for each application team member. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).
- B. Create an SCP and a permissions boundary for IAM roles. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.
- C. Put each AWS account in its own OU. Add an SCP to each OU to grant access to only the AWS services that the teams plan to use. Include conditions tn the AWS account of each team.
- D. Delegate application team leads to provision IAM rotes for each team. Conduct a quarterly review of the IAM rotes the team leads have provisioned. Ensure that the application team leads have the appropriate training to review IAM roles.

**Answer: B**

Explanation:
To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required:
Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization.
An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization.
SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see Service control policies overview.
Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see Permissions boundaries for IAM entities.

Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization. This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified.
Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access.
This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals.
The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible .
Verified Reference:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

**NEW QUESTION # 346**
A company has an AWS account that includes an Amazon S3 bucket. The S3 bucket uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all the objects at rest by using a customer managed key. The S3 bucket does not have a bucket policy.
An IAM role in the same account has an IAM policy that allows s3 List* and s3 Get' permissions for the S3 bucket. When the IAM role attempts to access an object in the S3 bucket the role receives an access denied message.
Why does the IAM rote not have access to the objects that are in the S3 bucket?

- A. The ACL of the S3 objects does not allow read access for the objects when the objects ace encrypted at rest.
- B. The IAM rote does not have permission to use the KMS CreateKey operation.
- C. The S3 bucket lacks a policy that allows access to the customer managed key that encrypts the objects.
- D. The IAM rote does not have permission to use the customer managed key that encrypts the objects that are in the S3 bucket.

**Answer: D**

Explanation:
When using server-side encryption with AWS KMS keys (SSE-KMS), the requester must have both Amazon S3 permissions and AWS KMS permissions to access the objects. The Amazon S3 permissions are for the bucket and object operations, such as s3:ListBucket and s3:GetObject. The AWS KMS permissions are for the key operations, such as kms:GenerateDataKey and kms:Decrypt. In this case, the IAM role has the necessary Amazon S3 permissions, but not the AWS KMS permissions to use the customer managed key that encrypts the objects. Therefore, the IAM role receives an access denied message when trying to access the objects. Verified References:
* https://docs.aws.amazon.com/AmazonS3/latest/userguide/troubleshoot-403-errors.html
* https://repost.aws/knowledge-center/s3-access-denied-error-kms
* https://repost.aws/knowledge-center/cross-account-access-denied-error-s3

**NEW QUESTION # 347**
A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs to make the application available to the vendors.
A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound direction. However, the vendors cannot connect to the application.
Which solution will provide the vendors access to the application?

- A. Modify the inbound rules on the internet gateway to allow the required ports.
- B. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.
- C. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
- D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

**Answer: C**

Explanation:
You must allow the ephemeral ports in the outbound NACL for the CIDR range.

**NEW QUESTION # 348**

A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.
Which solution will meet these requirements?

- A. In CloudTrail, turn on Insights events on the trail. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Configure a threshold of 3 and a period of 5 minutes.
- B. In AWS Identity and Access Management Access Analyzer, create a new analyzer. Configure the analyzer to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.
- C. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
- D. Create an Amazon Athena table from the CloudTrail events. Run a query for eventName matching ConsoleLogin and for errorMessage matching "Failed authentication". Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.

**Answer: C**

Explanation:
The correct answer is B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
This answer is correct because it meets the requirements of sending an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. By configuring CloudTrail to send events to CloudWatch Logs, the security engineer can create a metric filter that matches the desired pattern of failed sign-in events. Then, by creating a CloudWatch alarm based on the metric filter, the security engineer can set a threshold of 3 and a period of 5 minutes, and choose an action such as sending an email or an Amazon Simple Notification Service (Amazon SNS) message when the alarm is triggered12.
The other options are incorrect because:
A) Turning on Insights events on the trail and configuring an alarm on the insight is not a solution, because Insights events are used to analyze unusual activity in management events, such as spikes in API call volume or error rates. Insights events do not capture failed sign-in attempts to the AWS Management Console3.
C) Creating an Amazon Athena table from the CloudTrail events and running a query for failed sign-in events is not a solution, because it does not provide a mechanism to send an alert based on the query results. Amazon Athena is an interactive query service that allows analyzing data in Amazon S3 using standard SQL, but it does not support creating notifications or alarms from queries4.
D) Creating an analyzer in AWS Identity and Access Management Access Analyzer and configuring it to send an Amazon SNS notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes is not a solution, because IAM Access Analyzer is not a service that monitors sign-in events, but a service that helps identify resources that are shared with external entities. IAM Access Analyzer does not generate findings for failed sign-in attempts to the AWS Management Console5.
Reference:
1: Sending CloudTrail Events to CloudWatch Logs - AWS CloudTrail 2: Creating Alarms Based on Metric Filters - Amazon CloudWatch 3: Analyzing unusual activity in management events - AWS CloudTrail 4: What is Amazon Athena? - Amazon Athena 5: Using AWS Identity and Access Management Access Analyzer - AWS Identity and Access Management

**NEW QUESTION # 349**
......

In addition to the Amazon SCS-C02 PDF questions, we offer desktop AWS Certified Security - Specialty (SCS-C02) practice exam software and web-based AWS Certified Security - Specialty (SCS-C02) practice test to help applicants prepare successfully for the actual Building AWS Certified Security - Specialty (SCS-C02) exam. These AWS Certified Security - Specialty (SCS-C02) practice exams simulate the actual SCS-C02 exam conditions and provide an accurate assessment of test preparation.

**SCS-C02 Practice Exam Pdf**: https://www.testkingfree.com/Amazon/SCS-C02-practice-exam-dumps.html

- SCS-C02 Test Dumps Pdf □ SCS-C02 Free Exam □ SCS-C02 Interactive EBook □ Search for [ SCS-C02 ] on ➤ www.testsimulate.com □ immediately to obtain a free download □Reliable SCS-C02 Exam Pdf
- Quiz Amazon SCS-C02 AWS Certified Security - Specialty First-grade Reliable Dumps Questions □ The page for free download of ➡ SCS-C02 □□□ on ➠ www.pdfvce.com □ will open immediately □SCS-C02 Interactive EBook
- Reliable SCS-C02 Exam Syllabus □ Exam SCS-C02 Tests □ Certification SCS-C02 Exam Infor □ The page for free download of □ SCS-C02 □ on ➡ www.prep4pass.com □□□ will open immediately □Prep SCS-C02 Guide
- Download Updated Amazon SCS-C02 Exam Question and Start Preparation Today □ Open （ www.pdfvce.com ）

and search for □ SCS-C02 □ to download exam materials for free □Prep SCS-C02 Guide

- Dumps SCS-C02 Vce □ Pdf SCS-C02 Pass Leader □ Test SCS-C02 Engine Version □ （ www.examdiscuss.com ） is best website to obtain □ SCS-C02 □ for free download □Exam SCS-C02 Overviews
- 2025 Newest SCS-C02 – 100% Free Reliable Dumps Questions | AWS Certified Security - Specialty Practice Exam Pdf □ □ Easily obtain 「 SCS-C02 」 for free download through □ www.pdfvce.com □ □Real SCS-C02 Exam
- Amazon SCS-C02 Reliable Dumps Questions Exam Pass Certify | SCS-C02: AWS Certified Security - Specialty ～～ Open ➥ www.dumps4pdf.com □ enter □ SCS-C02 □ and obtain a free download □Pdf SCS-C02 Pass Leader
- SCS-C02 Pass4sure Torrent - SCS-C02 Valid Pdf - SCS-C02 Testking Exam □ Search for “ SCS-C02 ” and download it for free on ➠ www.pdfvce.com □ website □Pdf SCS-C02 Pass Leader
- SCS-C02 online test engine - SCS-C02 training study - SCS-C02 torrent dumps □ □ www.pdfdumps.com □ is best website to obtain ☀ SCS-C02 □☀□ for free download □Exam SCS-C02 Tests
- SCS-C02 Test Dumps Pdf □ Reliable SCS-C02 Exam Pdf □ Pdf SCS-C02 Pass Leader □ Search for 《 SCS-C02 》 and download it for free immediately on ➥ www.pdfvce.com □ □SCS-C02 Test Dumps Free
- Free PDF Quiz 2025 SCS-C02: AWS Certified Security - Specialty – High Pass-Rate Reliable Dumps Questions □ Download ☀ SCS-C02 □☀□ for free by simply entering [ www.pdfdumps.com ] website □Test SCS-C02 Dumps Free
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, hamadtrainingcenter.com, www.0317pk.com, www.fabu123.cyou, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by TestKingFree: https://drive.google.com/open?id=1COdJK6mIa-wnOtOUZoJ4u1SFFyQMIzRa