

# Amazon SCS-C02 Exam Actual Tests - SCS-C02 Latest Test Preparation



P.S. Free & New SCS-C02 dumps are available on Google Drive shared by Lead2PassExam: [https://drive.google.com/open?id=1990s4stANW6\\_IRZRIz4RYrF-Vc8v5YUV](https://drive.google.com/open?id=1990s4stANW6_IRZRIz4RYrF-Vc8v5YUV)

The content of our SCS-C02 exam questions emphasizes the focus and seizes the key to use refined SCS-C02 questions and answers to let the learners master the most important information by using the least amount of them. And we provide varied functions to help the learners learn our SCS-C02 Study Materials and prepare for the exam. The SCS-C02 self-learning and self-evaluation functions help the learners find their weak links and improve them promptly.

Even if you spend a small amount of time to prepare for SCS-C02 certification, you can also pass the exam successfully with the help of Lead2PassExam Amazon SCS-C02 braindump. Because Lead2PassExam exam dumps contain all questions you can encounter in the actual exam, all you need to do is to memorize these questions and answers which can help you 100% pass the exam. This is the royal road to Pass SCS-C02 Exam. Although you are busy working and you have not time to prepare for the exam, you want to get Amazon SCS-C02 certificate. At the moment, you must not miss Lead2PassExam SCS-C02 certification training materials which are your unique choice.

>> Amazon SCS-C02 Exam Actual Tests <<

## Amazon SCS-C02 Latest Test Preparation - Updated SCS-C02 Testkings

Passing the test SCS-C02 certification can help you realize your goal and find an ideal job. Buying our SCS-C02 latest question can help you pass the exam successfully. SCS-C02 exam question provides the free update and the discounts for the old client and our experts check whether our test bank has been updated on the whole day and if there is the update the system will send the update automatically to the client. Thus you can have an efficient learning and a good preparation of the exam. It is believed that our SCS-C02 latest question is absolutely good choices for you

### Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• Security Logging and Monitoring: This topic prepares AWS Security specialists to design and implement robust monitoring and alerting systems for addressing security events. It emphasizes troubleshooting logging solutions and analyzing logs to enhance threat visibility.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• 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.</li></ul>

## Amazon AWS Certified Security - Specialty Sample Questions (Q364-Q369):

### NEW QUESTION # 364

A company uses AWS Organizations and has many AWS accounts. The company has a new requirement to use server-side encryption with customer-provided keys (SSE-C) on all new object uploads to Amazon S3 buckets.

A security engineer is creating an SCP that includes a Deny effect for the s3:PutObject action.

Which condition must the security engineer add to the SCP to enforce the new SSE-C requirement?

- A. 

```
"Condition":{
  "Null":{
    "s3:x-amz-server-side-encryption-customer-algorithm": "true"
  }
}
```
- B. 

```
"Condition":{
  "StringNotEquals":{
    "s3:x-amz-server-side-encryption": "aws:kms"
  }
}
```
- C. 

```
"Condition":{
  "StringNotEquals":{
    "s3:x-amz-server-side-encryption-customer-algorithm": "AES256"
  }
}
```
- D. 

```
"Condition":{
  "Null":{
    "s3:x-amz-server-side-encryption": "true"
  }
}
```

**Answer: D**

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html#ssec-require-condition-key>

### NEW QUESTION # 365

A company has configured a gateway VPC endpoint in a VPC. Only Amazon EC2 instances that reside in a single subnet in the VPC can use the endpoint. The company has modified the route table for this single subnet to route traffic to Amazon S3 through the gateway VPC endpoint. The VPC provides internet access through an internet gateway.

A security engineer attempts to use instance profile credentials from an EC2 instance to retrieve an object from the S3 bucket, but the attempt fails. The security engineer verifies that the EC2 instance has an IAM instance profile with the correct permissions to access the S3 bucket and to retrieve objects. The security engineer also verifies that the S3 bucket policy is allowing access properly. Additionally, the security engineer verifies that the EC2 instance's security group and the subnet's network ACLs allow the communication.

What else should the security engineer check to determine why the request from the EC2 instance is failing?

- A. Verify that the EC2 instance's security group does not have an implicit inbound deny rule for Amazon S3.
- B. Verify that the internet gateway is allowing traffic to Amazon S3.
- C. Verify that the VPC endpoint policy is allowing access to Amazon S3.
- D. Verify that the VPC endpoint's security group does not have an explicit inbound deny rule for the EC2 instance.

**Answer: C**

Explanation:

Understanding Gateway VPC Endpoint:

A gateway VPC endpoint allows traffic from the VPC to specific AWS services (e.g., Amazon S3) without traversing the public internet.

Key Configuration Points to Verify:

The route table is correctly configured to send traffic for Amazon S3 through the gateway VPC endpoint.

IAM permissions and bucket policies are correct and allow access to the specific S3 bucket.

Verify the Endpoint Policy:

Check the VPC endpoint policy to ensure it allows access to the S3 bucket. The policy might be restricting access to certain buckets, prefixes, or IAM principals.

Example VPC Endpoint Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::example-bucket",
        "arn:aws:s3:::example-bucket/*"
      ]
    }
  ]
}
```

Testing and Validation:

Modify the endpoint policy if required and test access again from the EC2 instance.

Gateway VPC Endpoints Documentation

VPC Endpoint Policies for Amazon S3

### NEW QUESTION # 366

Your development team is using access keys to develop an application that has access to S3 and DynamoDB.

A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

- A. Delete the user associated with the keys after every 2 months. Then recreate the user again.
- B. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.
- C. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.
- D. Use the application to rotate the keys in every 2 months via the SDK

**Answer: C**

Explanation:

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.

The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list Option A is incorrect because you might as use a script for such maintenance activities Option C is incorrect because you would not rotate the users themselves Option D is incorrect because you don't use IAM roles for such a purpose For more information on the CLI command, please refer to the below Link:

<http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.html> The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

Submit your Feedback/Queries to our Experts

### NEW QUESTION # 367

A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected the company's business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.

The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.

A security engineer starts to enable access logging for the AWS WAF web ACLs.

What should the security engineer do next to meet these requirements with the MOST operational efficiency?

- A. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.
- B. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.
- **C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.**
- D. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.

**Answer: C**

Explanation:

The correct answer is C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

According to the AWS documentation<sup>1</sup>, AWS WAF offers logging for the traffic that your web ACLs analyze. The logs include information such as the time that AWS WAF received the request from your protected AWS resource, detailed information about the request, and the action setting for the rule that the request matched. You can send your logs to an Amazon CloudWatch Logs log group, an Amazon Simple Storage Service (Amazon S3) bucket, or an Amazon Kinesis Data Firehose.

To create a log analysis solution for the AWS WAF web ACLs, you can use Amazon Athena, which is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL<sup>2</sup>. You can use Athena to query and filter the AWS WAF logs by host or any other criteria. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

To use Athena with AWS WAF logs, you need to export the CloudWatch logs to an S3 bucket. You can do this by creating a subscription filter that sends your log events to a Kinesis Data Firehose delivery stream, which then delivers the data to an S3 bucket<sup>3</sup>. Alternatively, you can use AWS DMS to migrate your CloudWatch logs to S3<sup>4</sup>.

After you have exported your CloudWatch logs to S3, you can create a table in Athena that points to your S3 bucket and use the AWS service log format that matches your log schema<sup>5</sup>. For example, if you are using JSON format for your AWS WAF logs, you can use the AWSJSONSerDe serde. Then you can run SQL queries on your Athena table and filter the results by host or any other field in your log data.

Therefore, this solution meets the requirements of creating a log analysis solution for the AWS WAF web ACLs with the most operational efficiency. This solution does not require setting up any additional infrastructure or services, and it leverages the existing capabilities of CloudWatch, S3, and Athena.

The other options are incorrect because:

\* A. Specifying Amazon Redshift as the destination for the access logs is not possible, because AWS WAF does not support sending logs directly to Redshift. You would need to use an intermediate service such as Kinesis Data Firehose or AWS DMS to load the data from CloudWatch or S3 to Redshift.

Deploying the Amazon Athena Redshift connector is not necessary, because you can query Redshift data directly from Athena without using a connector<sup>6</sup>. This solution would also incur additional costs and operational overhead of managing a Redshift cluster.

\* B. Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon CloudWatch Logs Insights to design a query to filter the logs by host is not efficient or scalable.

CloudWatch Logs Insights is a feature that enables you to interactively search and analyze your log data

\* in CloudWatch Logs<sup>7</sup>. However, CloudWatch Logs Insights has some limitations, such as a maximum query duration of 20 minutes, a maximum of 20 log groups per query, and a maximum retention period of 24 months<sup>8</sup>. These limitations may affect your ability to perform complex and long-running analysis on your AWS WAF logs.

\* D. Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon Redshift Spectrum to query the logs and filter them by host is not efficient or cost-effective. Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of data in S3 without loading or transforming any data<sup>9</sup>. However, Redshift Spectrum requires a Redshift cluster to process the queries, which adds additional costs and operational overhead. Redshift Spectrum also charges you based on the number of bytes scanned by each query, which can be expensive if you have large volumes of log data<sup>10</sup>.

References:

1: Logging AWS WAF web ACL traffic - Amazon Web Services 2: What Is Amazon Athena? - Amazon Athena 3: Streaming CloudWatch Logs Data to Amazon S3 - Amazon CloudWatch Logs 4: Migrate data from CloudWatch Logs using AWS Database Migration Service - AWS Database Migration Service 5: Querying AWS service logs - Amazon Athena 6: Querying data from Amazon Redshift - Amazon Athena 7: Analyzing log data with CloudWatch Logs Insights - Amazon CloudWatch Logs 8: CloudWatch Logs Insights quotas - Amazon CloudWatch 9: Querying external data using Amazon Redshift Spectrum - Amazon Redshift 10:

Amazon Redshift Spectrum pricing - Amazon Redshift

### NEW QUESTION # 368

A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.

A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.

The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).

Which combination of steps should the security engineer take to gather this information? (Choose two.)

- A. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.
- B. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- C. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- D. Use Amazon OpenSearch Service to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.
- E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

Answer: A,B

### NEW QUESTION # 369

.....

As the quick development of the world economy and intense competition in the international, the world labor market presents many new trends: company's demand for the excellent people is growing. As is known to us, the SCS-C02 certification is one mainly mark of the excellent. If you want to improve your correct rates of exam, we believe the best method is inscribed according to the fault namely this in appearing weak sports, specific aim ground consolidates knowledge is nodded. Our SCS-C02 Guide Torrent will help you establish the error sets. We believe that it must be very useful for you to take your exam, and it is necessary for you to use our SCS-C02 test questions.

**SCS-C02 Latest Test Preparation:** <https://www.lead2passexam.com/Amazon/valid-SCS-C02-exam-dumps.html>

- Valid AWS Certified Security - Specialty exam, free latest Amazon SCS-C02 exam pdf  The page for free download of  SCS-C02  on  [www.troytecdumps.com](http://www.troytecdumps.com)  will open immediately  SCS-C02 Free Braindumps
- SCS-C02 Accurate Test  SCS-C02 Latest Exam Testking  Dump SCS-C02 Collection  The page for free download of  SCS-C02  on  [www.pdfvce.com](http://www.pdfvce.com)  will open immediately  SCS-C02 Accurate Test
- Get Useful SCS-C02 Exam Actual Tests and Pass Exam in First Attempt  Open website  [www.pdfdumps.com](http://www.pdfdumps.com)  and search for [ SCS-C02 ] for free download  SCS-C02 Free Braindumps
- SCS-C02 Latest Exam Testking  SCS-C02 Accurate Test  Reliable SCS-C02 Exam Papers  Search for  SCS-C02  on  [www.pdfvce.com](http://www.pdfvce.com)  immediately to obtain a free download  SCS-C02 Exam Tutorials
- Get Useful SCS-C02 Exam Actual Tests and Pass Exam in First Attempt  Go to website  [www.dumpsquestion.com](http://www.dumpsquestion.com)   open and search for  « SCS-C02 »  to download for free  Reliable SCS-C02 Mock Test
- Prepare with Amazon SCS-C02 PDF Questions [2026]-Best Preparation Materials  Enter  [www.pdfvce.com](http://www.pdfvce.com)  and search for  SCS-C02  to download for free  Dump SCS-C02 Collection
- Hot SCS-C02 Spot Questions  Complete SCS-C02 Exam Dumps  Test SCS-C02 Dumps Free  Search on  [www.troytecdumps.com](http://www.troytecdumps.com)  for  SCS-C02  to obtain exam materials for free download  Reliable SCS-C02 Exam Papers
- Hot SCS-C02 Spot Questions  SCS-C02 Accurate Test  Complete SCS-C02 Exam Dumps  Simply search for [ SCS-C02 ] for free download on { [www.pdfvce.com](http://www.pdfvce.com) }  Test SCS-C02 Dumps Free
- SCS-C02 Exam Tutorials  SCS-C02 Exam Tutorials  Dump SCS-C02 Collection  Search for  SCS-C02  and download it for free on  [www.practicevce.com](http://www.practicevce.com)  website  Hot SCS-C02 Spot Questions
- Latest SCS-C02 Test Dumps  SCS-C02 Instant Access  SCS-C02 Valid Torrent  « [www.pdfvce.com](http://www.pdfvce.com) »  is

best website to obtain “SCS-C02 ” for free download ☐Reliable SCS-C02 Exam Papers

- Up-to-Date Online Amazon SCS-C02 Practice Test Engine ☐ Download [ SCS-C02 ] for free by simply entering { [www.dumpsquestion.com](http://www.dumpsquestion.com) } website ☐Latest SCS-C02 Test Dumps
- [junaidijlr987179.bloggip.com](http://junaidijlr987179.bloggip.com), [thebookmarkage.com](http://thebookmarkage.com), [aadamsjpu149076.blog-eye.com](http://aadamsjpu149076.blog-eye.com), [mbtc.yipeily.cn](http://mbtc.yipeily.cn), [dac.husaen.com](http://dac.husaen.com), [gretaspkq316602.blognody.com](http://gretaspkq316602.blognody.com), [www.dibiz.com](http://www.dibiz.com), [bookmarkfox.com](http://bookmarkfox.com), [www.fuxinwang.com](http://www.fuxinwang.com), [lucykgnv249407.answerblogs.com](http://lucykgnv249407.answerblogs.com), Disposable vapes

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by Lead2PassExam: [https://drive.google.com/open?id=1990s4stANW6\\_IRZRLz4RYrF-Vc8v5YUV](https://drive.google.com/open?id=1990s4stANW6_IRZRLz4RYrF-Vc8v5YUV)