

AWS SCS-C02 Study Guide PDF

GRAB THE AWS SECURITY SPECIALTY CERTIFICATION PDF QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

SCS-C02

AWS Certified Security - Specialty

65 Questions Exam – 750 / 1000 Cut Score – Duration of 170 minutes

www.VMExam.com

Table of Contents

| | |
|--|---|
| Get an Overview of the SCS-C02 Certification:..... | 3 |
| Why Should You Earn the AWS SCS-C02 Certification? | 3 |
| What Is the AWS SCS-C02 Security Specialty Certification Exam Structure? | 3 |
| Enhance Knowledge with SCS-C02 Sample Questions: | 4 |
| What Study Guide Works Best in Acing the AWS SCS- C02 Security Specialty Certification? | 9 |
| Explore the Syllabus Topics and Learn from the Core: | 9 |
| Make Your Schedule: | 9 |
| Get Expert Advice from the Training: | 9 |
| Get Access to the PDF Sample Questions: | 9 |
| Avoid Dumps and Utilize the AWS SCS-C02 Practice Test: | 9 |

Get an Overview of the SCS-C02 Certification:

Who should take the [SCS-C02 exam](#)? This is the first question that comes to a candidate's mind when preparing for the Security Specialty certification. The SCS-C02 certification is suitable for candidates who are keen to earn knowledge on the Specialty and grab their AWS Certified Security - Specialty. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SCS-C02 study guide PDF is here to solve the problem. SCS-C02 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the AWS SCS-C02 Certification?

There are several reasons why one should grab the SCS-C02 certification.

- The Security Specialty certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the [AWS Certified Security - Specialty](#) is a powerful qualification for a prosperous career.

What Is the AWS SCS-C02 Security Specialty Certification Exam Structure?

| | |
|-------------------------------------|--|
| Exam Name | AWS Certified Security - Specialty (Security Specialty) |
| Exam Code | SCS-C02 |
| Exam Price | \$300 USD |
| Duration | 170 minutes |
| Number of Questions | 65 |
| Passing Score | 750 / 1000 |
| Recommended Training / Books | AWS Security Fundamentals (Second Edition) Security Engineering on AWS Exam Readiness - AWS Certified Security - Specialty |
| Schedule Exam | PEARSON VUE |
| Sample Questions | AWS SCS-C02 Sample Questions |
| Recommended Practice | AWS Certified Security - Specialty Practice Test |

Enhance Knowledge with SCS-C02 Sample Questions:

Question: 1

A company decides to place database hosts in its own VPC, and to set up VPC peering to different VPCs containing the application and web tiers. The application servers are unable to connect to the database.

Which network troubleshooting steps should be taken to resolve the issue? (Select TWO.)

- a) Check to see if the application servers are in a private subnet or public subnet.
- b) Check the route tables for the application server subnets for routes to the VPC peering connection.
- c) Check the NACLs for the database subnets for rules that allow traffic from the internet.
- d) Check the database security groups for rules that allow traffic from the application servers.
- e) Check to see if the database VPC has an internet gateway

Answer: b, d

Question: 2

A corporate cloud security policy states that communication 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) Add the `aws:sourceVpce` condition to the AWS KMS key policy referencing the company's VPC endpoint ID.
- 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) Create a VPC endpoint for AWS KMS with private DNS enabled.
- d) Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.
- e) Add the following condition to the AWS KMS key policy: `"aws:SourceIp": "10.0.0.0/16"`.

Answer: a, c

Question: 3

Why is it important to scan network logs?

- a) To keep an eye on what the employees on your network are doing.
- b) To ensure there are no dropped packets or high latency.
- c) To be alerted to unusual traffic entering and exiting your network as a potential security event.
- d) To know if access has been made to your private S3 buckets.

Answer: c

Question: 4

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information.

The Security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.

Which combination of steps would meet the requirements?

(Select TWO.)

- Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.
- Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
- Add a bucket policy that includes a deny if a PutObject request does not include `aws:SecureTransport`.
- Add a bucket policy with `aws:SourceIp` to allow uploads and downloads from the corporate intranet only.
- Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: b, c

Question: 5

A Security Engineer must set up security group rules for a three-tier application:

- Presentation tier – Accessed by users over the web, protected by the security group `presentation-sg`
- Logic tier – RESTful API accessed from the presentation tier through HTTPS, protected by the security group `logic-sg`
- Data tier – SQL Server database accessed over port 1433 from the logic tier, protected by the security group `data-sg`

Which combination of the following security group rules will allow the application to be secure and functional?

(Select THREE.)

- `presentation-sg`: Allow ports 80 and 443 from 0.0.0.0/0
- `data-sg`: Allow port 1433 from `presentation-sg`
- `data-sg`: Allow port 1433 from `logic-sg`
- `presentation-sg`: Allow port 1433 from `data-sg`
- `logic-sg`: Allow port 443 from `presentation-sg`
- `logic-sg`: Allow port 443 from 0.0.0.0/0

Answer: a, c, e

Question: 6

A company is hosting a web application on AWS and is using an Amazon S3 bucket to store images. Users should have the ability to read objects in the bucket. A Security Engineer has written the following bucket policy to grant public read access:

```
{
  "ID": "Policy1502987489630",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1502987487640",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::appbucket",
      "Principal": "*"
    }
  ]
}
```

Attempts to read an object, however, receive the error: "Action does not apply to any resource(s) in statement." What should the Engineer do to fix the error?

- Change the IAM permissions by applying PutBucketPolicy permissions.
- Verify that the policy has the same name as the bucket name. If not, make it the same.
- Change the resource section to "arn:aws:s3:::appbucket/*".
- Add an s3:ListBucket action.

Answer: c

Question: 7

A Security Engineer must ensure that all API calls are collected across all company accounts, and that they are preserved online and are instantly available for analysis for 90 days. For compliance reasons, this data must be restorable for 7 years.

Which steps must be taken to meet the retention needs in a scalable, cost-effective way?

- Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket with versioning enabled. Set a lifecycle policy to move the data to Amazon Glacier daily, and expire the data after 90 days.
- Enable AWS CloudTrail logging across all accounts to S3 buckets. Set a lifecycle policy to expire the data in each bucket after 7 years.
- Enable AWS CloudTrail logging across all accounts to Amazon Glacier. Set a lifecycle policy to expire the data after 7 years.
- Enable AWS CloudTrail logging across all accounts to a centralized Amazon S3 bucket. Set a lifecycle policy to move the data to Amazon Glacier after 90 days, and expire the data after 7 years.

Answer: d

Question: 8

A Security Engineer has been informed that a user's access key has been found on GitHub. The Engineer must ensure that this access key cannot continue to be used, and must assess whether the access key was used to perform any unauthorized activities.

Which steps must be taken to perform these tasks?

- a) Review the user's IAM permissions and delete any unrecognized or unauthorized resources.
- b) Delete the user, review Amazon CloudWatch Logs in all regions, and report the abuse.
- c) Delete or rotate the user's key, review the AWS CloudTrail logs in all regions, and delete any unrecognized or unauthorized resources.
- d) Instruct the user to remove the key from the GitHub submission, rotate keys, and re-deploy any instances that were launched.

Answer: c

Question: 9

An Application team is designing a solution with two applications. The Security team wants the applications' logs to be captured in two different places, because one of the applications produces logs with sensitive data.

Which solution meets the requirement with the LEAST risk and effort?

- a) Use Amazon CloudWatch Logs to capture all logs, write an AWS Lambda function that parses the log file, and move sensitive data to a different log.
- b) Use Amazon CloudWatch Logs with two log groups, with one for each application, and use an AWS IAM policy to control access to the log groups, as required.
- c) Aggregate logs into one file, then use Amazon CloudWatch Logs, and then design two CloudWatch metric filters to filter sensitive data from the logs.
- d) Add logic to the application that saves sensitive data logs on the Amazon EC2 instances' local storage, and write a batch script that logs into the Amazon EC2 instances and moves sensitive logs to a secure location.

Answer: b

Question: 10

When testing a new AWS Lambda function that retrieves items from an Amazon DynamoDB table, the Security Engineer notices that the function was not logging any data to Amazon CloudWatch Logs.

The following policy was assigned to the role assumed by the Lambda function:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Dynamo-1234567",
      "Action": [
```

```
"dynamodb:GetItem"
],
"Effect": "Allow",
"Resource": "*"
}
}
```

Which least-privilege policy addition would allow this function to log properly?

- a) {


```
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:*"
],
"Effect": "Allow"
}
```
- b) {


```
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogStream"
],
"Effect": "Allow"
}
```
- c) {


```
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents"
],
"Effect": "Allow"
}
```
- d) {


```
"Sid": "Logging-12345",
"Resource": "*",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogGroup",
"logs>DeleteLogStream",
"logs:getLogEvents",
"logs:PutLogEvents"
],
"Effect": "Allow"
}
```

Answer: c

What Study Guide Works Best in Acing the AWS SCS-C02 Security Specialty Certification?

The SCS-C02 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Security Specialty exam, getting in full touch of the [syllabus](#) is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the AWS SCS-C02 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a [PDF format](#) or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the AWS SCS-C02 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, SCS-C02 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven SCS-C02 Practice Test for Success!!!

Do you want to pass the SCS-C02 exam on your first attempt? Stop worrying; we, VMExam.com are here to provide you the best experience during your AWS Certified Security - Specialty preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium [SCS-C02 practice tests](#). Our expert-designed questions help you to improve performance and pass the exam on your first attempt.