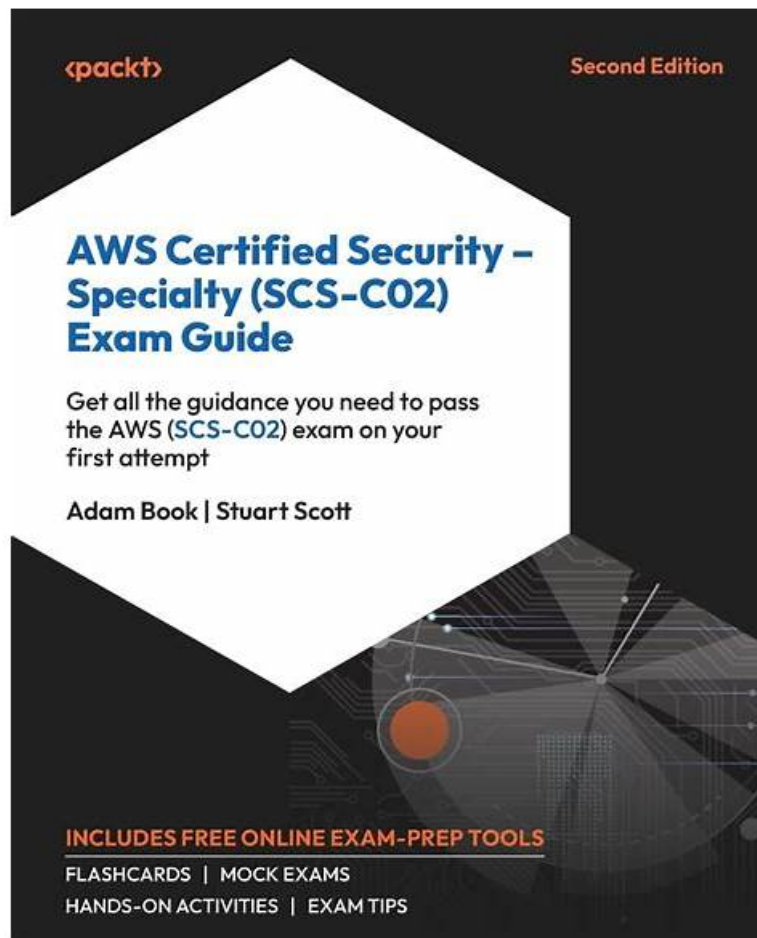


# SCS-C02 exam guide & SCS-C02 Real dumps & SCS-C02 free file



DOWNLOAD the newest TorrentValid SCS-C02 PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1IoqwGm--ZvRNtRXyYVSJBZ\\_zV2z-383b](https://drive.google.com/open?id=1IoqwGm--ZvRNtRXyYVSJBZ_zV2z-383b)

Our design and research on our SCS-C02 exam dumps are totally based on offering you the best help. We hope that learning can be a pleasant and relaxing process. If you really want to pass the SCS-C02 exam and get the certificate, just buy our SCS-C02 Study Guide. Our simulating exam environment will completely beyond your imagination. Your ability will be enhanced quickly. Let us witness the miracle of the moment!

## Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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>

Topic 3	<ul style="list-style-type: none"> <li>• <b>Identity and Access Management:</b> 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.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• <b>Security Logging and Monitoring:</b> 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 5	<ul style="list-style-type: none"> <li>• <b>Infrastructure Security:</b> Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.</li> </ul>

>> High SCS-C02 Quality <<

## The Best High SCS-C02 Quality & Authoritative Reliable SCS-C02 Test Review Ensure You a High Passing Rate

Services like quick downloading within five minutes, convenient and safe payment channels made for your convenience. Even newbies will be tricky about this process on the SCS-C02 exam questions. Unlike product from stores, quick browse of our SCS-C02 preparation quiz can give you the professional impression wholly. So, they are both efficient in practicing and downloading process. We also have free demo of SCS-C02 training guide as freebies for your reference to make your purchase more effective.

### Amazon AWS Certified Security - Specialty Sample Questions (Q367-Q372):

#### NEW QUESTION # 367

A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.

The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.

What could be the reason for the noncompliant status?

- A. The IAM credential report was generated within the past 4 hours.
- B. The security engineer does not have the GetCredentialReport permission.
- **C. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.**
- D. The security engineer does not have the GenerateCredentialReport permission.

**Answer: C**

Explanation:

The correct answer is D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

According to the AWS documentation<sup>1</sup>, the MaximumExecutionFrequency parameter specifies the maximum frequency with which AWS Config runs evaluations for a rule. For AWS Config managed rules, this value can be one of the following:

- \* One\_Hour
- \* Three\_Hours
- \* Six\_Hours
- \* Twelve\_Hours
- \* TwentyFour\_Hours

If the rule is triggered by configuration changes, it will still run evaluations when AWS Config delivers the configuration snapshot. However, if the rule is triggered periodically, it will not run evaluations more often than the specified frequency.

In this case, the security engineer enabled four AWS Config managed rules that are triggered periodically.

Therefore, these rules will only run evaluations every 24 hours, regardless of when the IAM credential report is generated. This means that the resources will display as noncompliant until the next evaluation cycle, which could take up to 24 hours after the IAM access keys are rotated.

The other options are incorrect because:

- \* A. The IAM credential report can be generated at any time, but it will not affect the compliance status of the resources until the next evaluation cycle of the AWS Config rules.
- \* B. The security engineer was able to invoke the IAM GenerateCredentialReport API operation, which means they have the GenerateCredentialReport permission. This permission is required to generate a credential report that lists all IAM users in an AWS account and their credential status.
- \* C. The security engineer does not need the GetCredentialReport permission to enable or evaluate AWS Config rules. This permission is required to retrieve a credential report that was previously generated by using the GenerateCredentialReport operation.

References:

1: AWS::Config::ConfigRule - AWS CloudFormation 2: IAM: Generate and retrieve IAM credential reports

### NEW QUESTION # 368

A company has enabled Amazon GuardDuty in all AWS Regions as part of its security monitoring strategy. In one of its VPCs, the company hosts an Amazon EC2 instance that works as an FTP server. A high number of clients from multiple locations contact the FTP server. GuardDuty identifies this activity as a brute force attack because of the high number of connections that happen every hour.

The company has flagged the finding as a false positive, but GuardDuty continues to raise the issue. A security engineer must improve the signal-to-noise ratio without compromising the company's visibility of potential anomalous behavior.

Which solution will meet these requirements?

- A. Create a suppression rule in GuardDuty to filter findings by automatically archiving new findings that match the specified criteria.
- B. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed.
- C. Create an AWS Lambda function that has the appropriate permissions to delete the finding whenever a new occurrence is reported.
- D. Add the FTP server to a trusted IP list. Deploy the list to GuardDuty to stop receiving the notifications.

**Answer: A**

Explanation:

"When you create an Amazon GuardDuty filter, you choose specific filter criteria, name the filter and can enable the auto-archiving of findings that the filter matches. This allows you to further tune GuardDuty to your unique environment, without degrading the ability to identify threats. With auto-archive set, all findings are still generated by GuardDuty, so you have a complete and immutable history of all suspicious activity."

### NEW QUESTION # 369

During a manual review of system logs from an Amazon Linux EC2 instance, a Security Engineer noticed that there are sudo commands that were never properly alerted or reported on the Amazon CloudWatch Logs agent. Why were there no alerts on the sudo commands?

- A. CloudWatch Logs status is set to ON versus SECURE, which prevents it from pulling in OS security event logs
- B. The VPC requires that all traffic go through a proxy, and the CloudWatch Logs agent does not support a proxy configuration.
- C. There is a security group blocking outbound port 80 traffic that is preventing the agent from sending the logs
- D. The IAM instance profile on the EC2 instance was not properly configured to allow the CloudWatch Logs agent to push the logs to CloudWatch

**Answer: D**

### NEW QUESTION # 370

A company wants to start processing sensitive data on Amazon EC2 instances. The company will use Amazon CloudWatch Logs to monitor, store, and access log files from the EC2 instances.

The company's developers use CloudWatch Logs for troubleshooting. A security engineer must implement a solution that prevents the developers from viewing the sensitive data. The solution must automatically apply to any new log groups that are created in the account in the future.

Which solution will meet these requirements?

- A. Create a CloudWatch Logs data protection policy for each log group. Specify the appropriate data identifiers for the policy. Ensure that the developers do not have the logs:Unmask IAM permission.
- B. Export the CloudWatch Logs data to an Amazon S3 bucket. Set up automated discovery by using Amazon Macie on the S3 bucket. Create a custom data identifier for the sensitive data. Remove the developers' access to CloudWatch Logs. Grant permissions for the developers to view the exported log data in Amazon S3.
- C. Export the CloudWatch Logs data to an Amazon S3 bucket. Set up automated discovery by using Amazon Macie on the S3 bucket. Specify the appropriate managed data identifiers. Remove the developers' access to CloudWatch Logs. Grant permissions for the developers to view the exported log data in Amazon S3.
- **D. Create a CloudWatch Logs account-wide data protection policy. Specify the appropriate data identifiers for the policy. Ensure that the developers do not have the logs:Unmask IAM permission.**

**Answer: D**

### NEW QUESTION # 371

A healthcare company has multiple AWS accounts in an organization in AWS Organizations. The company uses Amazon S3 buckets to store sensitive information of patients. The company needs to restrict users from deleting any S3 bucket across the organization.

What is the MOST scalable solution that meets these requirements?

- A. Permissions boundaries in AWS Identity and Access Management (IAM)
- B. S3 bucket policies
- C. Tag policies
- **D. SCPs**

**Answer: D**

Explanation:

AWS Organizations and SCPs:

SCPs allow centralized control over permissions across all accounts in an AWS Organization.

Use SCPs to prevent specific actions, such as S3 bucket deletion, across all accounts.

Create an SCP for S3 Bucket Deletion:

Define an SCP that explicitly denies the s3:DeleteBucket action.

Example SCP:

```
{
"Version": "2012-10-17",
"Statement":
[
{
"Effect": "Deny",
"Action": "s3:DeleteBucket",
"Resource": "*"
}
]
}
```

Attach SCP to the Root or Specific OUs:

Attach the SCP to the root of the organization or specific organizational units (OUs) as needed.

Advantages:

Scalability: Applies to all accounts in the organization without the need for individual configuration.

Compliance: Ensures sensitive S3 buckets are protected from accidental or malicious deletion.

AWS Organizations SCP Documentation

Restricting S3 Actions with SCPs

### NEW QUESTION # 372

.....

The Amazon SCS-C02 Certification Exam is one of the top-rated career advancement certifications in the market. With the AWS Certified Security - Specialty SCS-C02 certification exam everyone can validate their skills and knowledge after passing the SCS-C02 text. The Amazon AWS Certified Security - Specialty certification exam will recognize your expertise and knowledge in the market. You will get solid proof of your proven skill set. There are other countless benefits that you can gain after passing the

