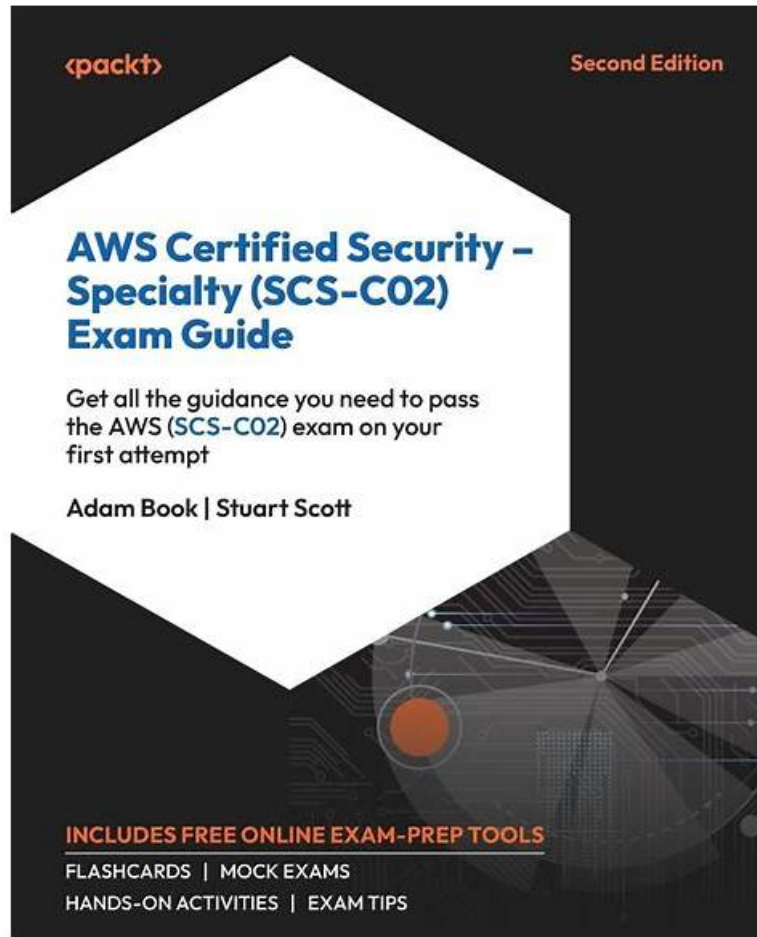


# Amazon SCS-C02 Exam | SCS-C02 Reliable Test Prep - Spend your Little Time and Energy to Prepare for SCS-C02



BTW, DOWNLOAD part of PracticeDump SCS-C02 dumps from Cloud Storage: <https://drive.google.com/open?id=17pWrtCrGrRgsGXadryiCl68h-zM633hq>

In modern society, innovation is of great significance to the survival of a company. The new technology of the SCS-C02 study materials is developing so fast. So the competitiveness among companies about the study materials is fierce. Luckily, our company masters the core technology of developing the AWS Certified Security - Specialty study materials. No company in the field can surpass us. So we still hold the strong strength in the market. At present, our SCS-C02 study materials have applied for many patents. We attach great importance on the protection of our intellectual property. What is more, our research center has formed a group of professional experts responsible for researching new technology of the SCS-C02 Study Materials. The technology of the SCS-C02 study materials will be innovated every once in a while. As you can see, we never stop innovating new version of the SCS-C02 study materials. We really need your strong support.

Once you start to become diligent and persistent, you will be filled with enthusiasms. Nothing can defeat you as long as you are optimistic. We sincerely hope that our SCS-C02 study materials can become your new purpose. Our SCS-C02 study materials can teach you much practical knowledge, which is beneficial to your career development. In order to survive in the society and realize our own values, learning our SCS-C02 Study Materials is the best way. Never stop improving yourself. The society warmly welcomes struggling people.

>> SCS-C02 Reliable Test Prep <<

**SCS-C02 Clearer Explanation, Exam SCS-C02 Success**

You will get multiple excellent offers if you buy Amazon SCS-C02 actual exam dumps today. We offer up to three months of free AWS Certified Security - Specialty Expert SCS-C02 exam questions updates. If the Amazon SCS-C02 real exam content changes within three months of your purchase, we will provide you with free valid Amazon SCS-C02 Dumps updates. Additionally, you can test the specifications of our SCS-C02 PDF questions file and Amazon Campaign Certification SCS-C02 practice test exams by trying free demos. Purchase this updated Amazon SCS-C02 practice test material today with all these amazing offers.

## Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>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.</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>Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.</li> </ul>

## Amazon AWS Certified Security - Specialty Sample Questions (Q147-Q152):

### NEW QUESTION # 147

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Place the security appliance in the public subnet with the internet gateway
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Configure the security appliance's elastic network interface for promiscuous mode.

**Answer: C**

Explanation:

Explanation

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#eni-basics> Source/destination checking "You must disable source/destination checks if the instance runs services such as network address translation, routing, or firewalls." The correct answer is C. Disable the Network Source/Destination check on the security appliance's elastic network interface.

This answer is correct because disabling the Network Source/Destination check allows the virtual security appliance to route traffic that is not addressed to or from itself. By default, this check is enabled on all EC2 instances, and it prevents them from forwarding traffic that does not match their own IP or MAC addresses.

However, for a virtual security appliance that acts as a router or a firewall, this check needs to be disabled, otherwise it will drop the traffic that it is supposed to route<sup>1</sup>2.

The other options are incorrect because:

A: Disabling network ACLs is not a solution, because network ACLs are optional layers of security for the subnets in a VPC. They can be used to allow or deny traffic based on IP addresses and ports, but they do not affect the routing behavior of the virtual security appliance<sup>3</sup>.

B; Configuring the security appliance's elastic network interface for promiscuous mode is not a solution, because promiscuous mode is a mode for a network interface that causes it to pass all traffic it receives to the CPU, rather than passing only the frames that it is programmed to receive. Promiscuous mode is normally used for packet sniffing or monitoring, but it does not enable the network interface to route traffic<sup>4</sup>.

D: Placing the security appliance in the public subnet with the internet gateway is not a solution, because it does not address the

routing issue of the virtual security appliance. The security appliance can be placed in either a public or a private subnet, depending on the network design and security requirements, but it still needs to have the Network Source/Destination check disabled to route traffic properly<sup>5</sup>.

References:

1: Enabling or disabling source/destination checks - Amazon Elastic Compute Cloud 2: Virtual security appliance - Wikipedia 3: Network ACLs - Amazon Virtual Private Cloud 4: Promiscuous mode - Wikipedia 5: NAT instances - Amazon Virtual Private Cloud

### NEW QUESTION # 148

A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way?

`{resolve:s3:MyBucketName:MyObjectName}` }.

- A. Store the API key value in Amazon DynamoDB. In the template, replace all references to the value with `{{resolve:dynamodb:MyTableName:MyPrimaryKey}}` }.
- **B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with `{resolve:secretsmanager:MySecretId:SecretString}` }.**
- C. Store the API key value in a new Amazon S3 bucket. In the template, replace all references to the value with `{resolve:s3:MyBucketName:MyObjectName}` }.
- D. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store. In the template, replace all references to the value with `{{resolve:ssm:MySSMParameterName:I}}` }.

**Answer: B**

Explanation:

Explanation

The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with `{{resolve:secretsmanager:MySecretId:SecretString}}` }.

This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle<sup>1</sup>. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the

`{{resolve:secretsmanager:...}}` } syntax<sup>2</sup>. This way, you can avoid exposing your secrets in plaintext and still use them in your resources.

The other options are incorrect because:

A: Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters.

This means that you cannot use the `{{resolve:ssm:...}}` } syntax to retrieve encrypted parameter values from Parameter Store<sup>3</sup>. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.

C: Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the

`{{resolve:dynamodb:...}}` } syntax to retrieve item values from DynamoDB tables<sup>4</sup>. You would have to use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.

D: Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the

`{{resolve:s3:...}}` } syntax to retrieve object values from S3 buckets<sup>5</sup>. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.

References:

1: What is AWS Secrets Manager? 2: Referencing AWS Secrets Manager secrets from Parameter Store parameters 3: Using dynamic references to specify template values 4: Amazon DynamoDB 5: Amazon Simple Storage Service (S3)

### NEW QUESTION # 149

A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).

The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront

receives the request from IAM WAF and then uses the ALB as the distribution's origin.

During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.

How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

- A. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.
- B. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
- **C. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.**
- D. Configure the CloudFront distribution to use the Lambda@Edge feature. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer requests. Block the request if the rate limit is exceeded.

**Answer: C**

### NEW QUESTION # 150

A company uses AWS Organizations. The company wants to implement short-term credentials for third-party AWS accounts to use to access accounts within the company's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.

Which solution will meet these requirements?

- **A. Create a unique IAM role for each external account. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.**
- B. Create a unique IAM role for each external account. Create a trust policy. Use AWS Secrets Manager to create a random external key.
- C. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.
- D. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identity source of choice. Grant access to users and groups from other accounts by using permission sets that are assigned by account.

**Answer: A**

Explanation:

Explanation

The correct answer is D.

To implement short-term credentials for third-party AWS accounts, you can use IAM roles and trust policies.

A trust policy is a JSON policy document that defines who can assume the role. You can specify the AWS account ID of the third-party account as a principal in the trust policy, and use the sts:ExternalId condition key to enhance the security of the role. The sts:ExternalId condition key is a unique identifier that is agreed upon by both parties and included in the AssumeRole request. This way, you can prevent the "confused deputy" problem, where an unauthorized party can use the same role as a legitimate party.

Option A is incorrect because bearer token authentication with OAuth or SAML is not suitable for granting access to AWS accounts and resources. Amazon Cognito and API Gateway are used for building web and mobile applications that require user authentication and authorization.

Option B is incorrect because AWS IAM Identity Center (AWS Single Sign-On) is a service that simplifies the management of access to multiple AWS accounts and cloud applications for your workforce users. It does not support granting access to third-party AWS accounts.

Option C is incorrect because using AWS Secrets Manager to create a random external key is not necessary and adds operational complexity. You can use the sts:ExternalId condition key instead to provide a unique identifier for each external account.

### NEW QUESTION # 151

An audit determined that a company's Amazon EC2 instance security group violated company policy by allowing unrestricted incoming SSH traffic. A security engineer must implement a near-real-time monitoring and alerting solution that will notify administrators of such violations.

Which solution meets these requirements with the MOST operational efficiency?

- **A. Use the restricted-ssh IAM Config managed rule that is invoked by security group configuration changes that are not compliant. Use the IAM Config remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.**
- B. Create a recurring Amazon Inspector assessment run that runs every day and uses the Security Best Practices package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the

Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

- C. Configure VPC Flow Logs for the VPC, and specify an Amazon CloudWatch Logs group. Subscribe the CloudWatch Logs group to an IAM Lambda function that parses new log entries, detects successful connections on port 22, and publishes a notification through Amazon Simple Notification Service (Amazon SNS).
- D. Create a recurring Amazon Inspector assessment run that runs every day and uses the Network Reachability package. Create an Amazon CloudWatch rule that invokes an IAM Lambda function when an assessment run starts. Configure the Lambda function to retrieve and evaluate the assessment run report when it completes. Configure the Lambda function also to publish an Amazon Simple Notification Service (Amazon SNS) notification if there are any violations for unrestricted incoming SSH traffic.

**Answer: A**

Explanation:

The most operationally efficient solution to implement a near-real-time monitoring and alerting solution that will notify administrators of security group violations is to use the restricted-ssh AWS Config managed rule that is invoked by security group configuration changes that are not compliant. This rule checks whether security groups that are in use have inbound rules that allow unrestricted SSH traffic. If a violation is detected, AWS Config can use the remediation feature to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.

Option A is incorrect because creating a recurring Amazon Inspector assessment run that uses the Network Reachability package is not operationally efficient, as it requires setting up an assessment target and template, running the assessment every day, and invoking a Lambda function to retrieve and evaluate the assessment report. It also does not provide near-real-time monitoring and alerting, as it depends on the frequency and duration of the assessment run.

Option C is incorrect because configuring VPC Flow Logs for the VPC and specifying an Amazon CloudWatch Logs group is not operationally efficient, as it requires creating a log group and stream, enabling VPC Flow Logs for each subnet or network interface, and subscribing a Lambda function to parse and analyze the log entries. It also does not provide proactive monitoring and alerting, as it only detects successful connections on port 22 after they have occurred.

Option D is incorrect because creating a recurring Amazon Inspector assessment run that uses the Security Best Practices package is not operationally efficient, for the same reasons as option A. It also does not provide specific monitoring and alerting for security group violations, as it covers a broader range of security issues. Reference:

[AWS Config Rules]

[AWS Config Remediation]

[Amazon Inspector]

[VPC Flow Logs]

## NEW QUESTION # 152

.....

Your personal experience will defeat all advertisements that we post before. When you enter our website, you can download the free demo of SCS-C02 exam software. We believe you will like our dumps that have helped more candidates Pass SCS-C02 Exam after you have tried it. Using our exam dump, you can easily become IT elite with SCS-C02 exam certification.

**SCS-C02 Clearer Explanation:** [https://www.practicedump.com/SCS-C02\\_actualtests.html](https://www.practicedump.com/SCS-C02_actualtests.html)

- Free PDF 2026 First-grade Amazon SCS-C02: AWS Certified Security - Specialty Reliable Test Prep  Immediately open [www.examdiscuss.com](http://www.examdiscuss.com)  and search for [SCS-C02](#)   to obtain a free download  Exam Cram SCS-C02 Pdf
- Reliable SCS-C02 Exam Prep  Download SCS-C02 Demo  SCS-C02 Latest Test Practice  Simply search for [SCS-C02](#)  for free download on  [www.pdfvce.com](http://www.pdfvce.com)   Reliable SCS-C02 Exam Simulator
- Pass Guaranteed 2026 Marvelous Amazon SCS-C02: AWS Certified Security - Specialty Reliable Test Prep  Go to website [www.vceengine.com](http://www.vceengine.com)  open and search for [SCS-C02](#)  to download for free  Test SCS-C02 Questions Fee
- Verified SCS-C02 Reliable Test Prep Spend Your Little Time and Energy to Pass Amazon SCS-C02 exam  Enter  [www.pdfvce.com](http://www.pdfvce.com)   and search for [SCS-C02](#)  to download for free  Reliable SCS-C02 Exam Prep
- Reliable SCS-C02 Exam Prep  SCS-C02 Certification Cost  SCS-C02 Reliable Study Questions  Search for [SCS-C02](#)  and download it for free immediately on  [www.vce4dumps.com](http://www.vce4dumps.com)   SCS-C02 Exam Voucher
- Free PDF Amazon - SCS-C02 - High Hit-Rate AWS Certified Security - Specialty Reliable Test Prep  Search for  SCS-C02  and download exam materials for free through  [www.pdfvce.com](http://www.pdfvce.com)   Reliable SCS-C02 Exam Simulator
- SCS-C02 Real Questions  SCS-C02 Latest Test Practice  Reliable SCS-C02 Exam Prep  Copy URL

[www.examcollectionpass.com](http://www.examcollectionpass.com) open and search for ➔ SCS-C02 to download for free Certificate SCS-C02 Exam

- SCS-C02 Study Questions - AWS Certified Security - Specialty Guide Torrent -amp; SCS-C02 Exam Torrent Search for 【 SCS-C02 】 and download it for free immediately on [www.pdfvce.com](http://www.pdfvce.com) SCS-C02 Reliable Exam Practice
- Valid SCS-C02 Exam Camp Pdf Latest SCS-C02 Test Testking Latest SCS-C02 Test Testking Search for [ SCS-C02 ] on [www.examdiscuss.com](http://www.examdiscuss.com) immediately to obtain a free download Test SCS-C02 Questions Fee
- Real and Updated SCS-C02 Exam Questions Search for SCS-C02 and download exam materials for free through [www.pdfvce.com](http://www.pdfvce.com) Reliable SCS-C02 Exam Simulator
- Valid SCS-C02 Exam Topics Latest SCS-C02 Test Testking Latest SCS-C02 Test Testking Search for SCS-C02 and obtain a free download on ➔ [www.prep4sures.top](http://www.prep4sures.top) SCS-C02 Exam Voucher
- [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [emiliaizwy839235.blog4youth.com](http://emiliaizwy839235.blog4youth.com), [robertoybw559741.tkzblog.com](http://robertoybw559741.tkzblog.com), [kiarasisf787286.blogdosaga.com](http://kiarasisf787286.blogdosaga.com), [rebeccarout798722.blog-kids.com](http://rebeccarout798722.blog-kids.com), [rajanpebi920371.newsblgger.com](http://rajanpebi920371.newsblgger.com), [janeojdx692424.blogthisbiz.com](http://janeojdx692424.blogthisbiz.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [bookmarkinglive.com](http://bookmarkinglive.com), Disposable vapes

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by PracticeDump: <https://drive.google.com/open?id=17pWrtCrGrRgsGXadryiCl68h-zM633hq>