# SCS-C02 Certification Torrent, Reliable SCS-C02 Exam Materials


DOWNLOAD the newest FreePdfDump SCS-C02 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1tUbEx-2gQuKQG-i5OON38LMu5p8xP2HG

It is not a time to get scared of taking any difficult certification exam such as SCS-C02. The excellent study guides, practice questions and answers and dumps offered by FreePdfDump are your real strength to take the test with confidence and pass it without facing any difficulty. Passing an SCS-C02 exam rewards you in the form of best career opportunities. A profile rich with relevant credentials opens up a number of career slots in major enterprises. FreePdfDump's SCS-C02 Questions and answers based study material guarantees you career heights by helping you pass as many exams as you want.

## Amazon SCS-C02 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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 2 | • Infrastructure Security: 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. |
| Topic 3 | • 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. |
| Topic 4 | • 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. |
| Topic 5 | • 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 Certification Torrent <<**

# Trustable SCS-C02 Certification Torrent Help You to Get Acquainted with Real SCS-C02 Exam Simulation

It is never too late to try new things no matter how old you are. Someone always give up their dream because of their ages, someone give up trying to overcome SCS-C02 exam because it was difficult for them. Now, no matter what the reason you didn't pass the exam, our study materials will try our best to help you. If you are not sure what kinds of SCS-C02 Exam Question is appropriate for you, you can try our free demo of the PDF version. There must be one that suits you best. Your life will become more meaningful because of your new change, and our SCS-C02 question torrents will be your first step.

## Amazon AWS Certified Security - Specialty Sample Questions (Q400-Q405):

**NEW QUESTION # 400**
An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet. TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.
What should a security engineer do to meet these requirements?

- A. Create a public Network Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.
- B. Create a public Application Load Balancer. Create two listeners: one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.
- C. Create a public Network Load Balancer. Create a listener on port 443. Create one target group.Create a rule to forward traffic from port 443 to the target group. Set the protocol for the listener on port 443 to TLS.
- D. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.

**Answer: B**

Explanation:
The security engineer should create a public Application Load Balancer, create two listeners (one on port 80 and one on port 443), create one target group, and create a rule to forward traffic from port 80 to the listener on port 443. Then, they should provision a public TLS certificate in AWS Certificate Manager (ACM) and attach the certificate to the listener on port 443. This setup will implement TLS for incoming traffic to the application, without requiring an end-to-end configuration.

**NEW QUESTION # 401**
An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance. The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.
What should a security engineer do to meet these requirements?

- A. Create a public Network Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.
- B. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.
- C. Create a public Application Load Balancer. Create two listeners one listener on port 80 and one listener on port 443. Create one target group. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.
- D. Create a public Network Load Balancer. Create a listener on port 443. Create one target group. Create a rule to forward traffic from port 443 to the target group. Set the protocol for the listener on port 443 to TLS.

**Answer: C**

Explanation:
An Application Load Balancer (ALB) is a type of load balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic based on the content of the request, such as the host header, path, or query parameters. An ALB can also terminate TLS connections and decrypt requests from clients before sending them to the targets.
To implement TLS for incoming traffic to the application, the following steps are required:
Create a public ALB in a public subnet and register the EC2 instances as targets in a target group.
Create two listeners for the ALB, one on port 80 for HTTP traffic and one on port 443 for HTTPS traffic.
Create a rule for the listener on port 80 to redirect HTTP requests to HTTPS using the same host, path, and query parameters.
Provision a public TLS certificate in AWS Certificate Manager (ACM) for the domain name of the application. ACM is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources.
Attach the certificate to the listener on port 443 and configure the security policy to negotiate secure connections between clients and the ALB.
Configure the security groups for the ALB and the EC2 instances to allow inbound traffic on ports 80 and 443 from the internet and outbound traffic on any port to the EC2 instances.
This solution will meet the requirements of implementing TLS for incoming traffic without impacting performance or requiring end-to-end encryption. The ALB will handle the TLS termination and decryption, while forwarding unencrypted requests to the EC2 instances.
Verified Reference:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html
https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

**NEW QUESTION # 402**
A company is using IAM Secrets Manager to store secrets for its production Amazon RDS database. The Security Officer has asked that secrets be rotated every 3 months. Which solution would allow the company to securely rotate the secrets? (Select TWO.)

- A. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Configure the private subnet to use a NAT gateway. Schedule the Lambda function to run every 3 months to rotate the secrets.
- B. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Schedule the Lambda function to run quarterly to rotate the secrets.
- C. Place the RDS instance in a private subnet and an IAM Lambda function inside the VPC in the private subnet. Configure a Secrets Manager interface endpoint. Schedule the Lambda function to run every 3 months to rotate the secrets.
- D. Place the RDS instance in a public subnet and an IAM Lambda function outside the VPC. Schedule the Lambda function to run every 3 months to rotate the secrets.
- E. Place the RDS instance in a private subnet and an IAM Lambda function outside the VPC. Configure the private subnet to use an internet gateway. Schedule the Lambda function to run every 3 months lo rotate the secrets.

**Answer: A,C**

Explanation:
these are the solutions that can securely rotate the secrets for the production RDS database using Secrets Manager. Secrets Manager is a service that helps you manage secrets such as database credentials, API keys, and passwords. You can use Secrets Manager to rotate secrets automatically by using a Lambda function that runs on a schedule. The Lambda function needs to have access to both the RDS instance and the Secrets Manager service. Option B places the RDS instance in a private subnet and the Lambda function in the same VPC in another private subnet. The private subnet with the Lambda function needs to use a NAT gateway to access Secrets Manager over the internet. Option E places the RDS instance and the Lambda function in the same private subnet and configures a Secrets Manager interface endpoint, which is a private connection between the VPC and Secrets Manager. The other options are either insecure or incorrect for rotating secrets using Secrets Manager.

**NEW QUESTION # 403**
A security engineer for a large company is managing a data processing application used by 1.500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidianes and should not be available on the public internet. To meet the compliance requirements for restricted access, the engineer has received the public and private

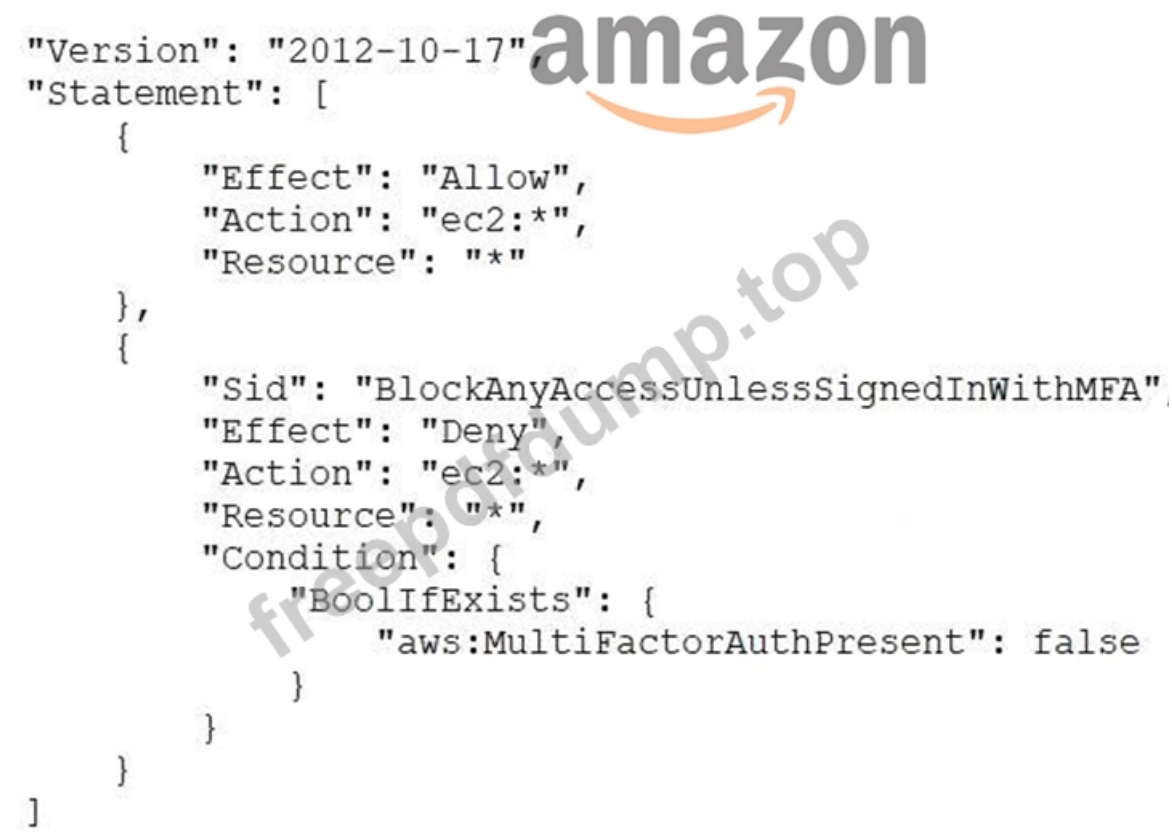
CIDR block ranges for each subsidiary.
What solution should the engineer use to implement the appropriate access restrictions for the application?

- A. Create an AWS PrivateLink endpoint service in the parent company account attached to the NLB.
  Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoint Use AWS PrivateLink interface endpoints in the 1.500 subsidiary AWS accounts to connect to the data processing application.
- B. Create an AWS security group to allow access on TCP port 443 from the 1.500 subsidiary CIDR block ranges.
  Associate the security group with EC2 instances.
- C. Create a NACL to allow access on TCP port 443 (rom the 1.500 subsidiary CIDR block ranges Associate the NACL to both the NLB and EC2 instances.
- D. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges Associate the security group to the NLB Create a second security group (or EC2 instances with access on TCP port 443 from the NLB security group.

**Answer: A**

Explanation:
* Requirement Analysis:
* The application should only be accessible to subsidiary companies over TCP port 443.
* Direct public internet access must be restricted.
* Use AWS PrivateLink:
* AWS PrivateLink allows secure access to services across accounts and VPCs without exposing them to the public internet.
* Steps to Implement:
* Parent Account:
* Create aPrivateLink Endpoint Servicelinked to the Network Load Balancer (NLB).
* Update the security group for the EC2 instances to allow traffic from the PrivateLink endpoint on TCP port 443.
* Subsidiary Accounts:
* CreateInterface Endpointsin the subsidiary VPCs. These endpoints securely route traffic to the parent company's application via PrivateLink.
* Advantages of This Solution:
* Compliance: Ensures secure communication without internet exposure.
* Scalability: Easily supports all 1,500 subsidiaries.
* Operational Simplicity: Centralized service in the parent account, while subsidiaries connect securely via endpoints.
AWS PrivateLink Documentation
Using Security Groups with AWS PrivateLink

**NEW QUESTION # 404**
An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:




After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI.
What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and --token-code parameters. Use these resulting values to make API /CLI calls.
- B. Change the value of aws:MultiFactorAuthPresent to true.
- C. Create a role and enforce multi-factor authentication in the role trust policy. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameters. Store the resulting values in environment variables. Add sts:AssumeRole to NotAction in the policy.
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.

**Answer: A**

Explanation:
The correct answer is B. Instruct users to run the aws sts get-session-token CLI command and pass the multi- factor authentication --serial-number and --token-code parameters. Use these resulting values to make API /CLI calls.
According to the AWS documentation1, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.
You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the get- session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error.
The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.
Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.
The other options are incorrect because:
* A. Changing the value of aws:MultiFactorAuthPresent to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA

information to AWS for this condition key to be true.
* C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the get-session-token command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.
* D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the get-session-token command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the sts assume-role command instead of the get-session-token command.
References:
1: get-session-token - AWS CLI Command Reference

**NEW QUESTION # 405**
.....

The service of SCS-C02 test guide is very prominent. It always considers the needs of customers in the development process. There are three versions of our SCS-C02 learning question, PDF, PC and APP. You can choose according to your needs. Of course, you can use the trial version of SCS-C02 exam training in advance. After you use it, you will have a more profound experience. You can choose your favorite our SCS-C02 Study Materials version according to your feelings. I believe that you will be more inclined to choose a good service product, such as SCS-C02 learning question