SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/aws-certified-security-specialty.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure AWS WAF rules to implement the required rules.

B. Use the operating system built-in, host-based firewall to implement the required rules.

C. Use a NAT gateway to control ingress and egress according to the requirements.

D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

Correct Answer: B

QUESTION 2

A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be

rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

Please select:

A. Enable automatic key rotation for a CMK

B. Import new key material to an existing CMK

C. Use the CLI or console to explicitly rotate an existing CMK

D. Import new key material to a new CMK; Point the key alias to the new CMK.

E. Delete an existing CMK and a new default CMK will be created.

Correct Answer: AD

The AWS Documentation mentions the following Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually. Rotating Keys Manually You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation. When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK. Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html The correct

answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.

QUESTION 3

A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out. No changes have been made to the response plan have been made since its creation. Which of the following is a right statement with regards to the plan?

Please select:

A. It places too much emphasis on already implemented security controls.

B. The response plan is not implemented on a regular basis

C. The response plan does not cater to new services

D. The response plan is complete in its entirety

Correct Answer: C

So definitely the case here is that the incident response plan is not catering to newly created services. AWS keeps on changing and adding new services and hence the response plan must cater to these new services. Option A and B are invalid because we don\\'t know this for a fact. Option D is invalid because we know that the response plan is not complete, because it does not cater to new features of AWS For more information on incident response plan please visit the following URL: https://aws.amazon.com/blogs/publicsector/buildins-a-cloud-specific-incident-response-plan; The correct answer is: The response plan does not cater to new services

QUESTION 4

A company has an AWS Lambda function that requires access to an Amazon S3 bucket. The company\\'s security policy requires that connections to Amazon S3 are over a private network and are secure.

The company has configured a gateway VPC endpoint in the VPC to allow access to Amazon S3. The company has configured the Lambda function to run inside the VPC. Additionally, the company has configured the Lambda function to use

a private subnet that has a route to the internet through a NAT gateway.

Other resources in the VPC use this private subnet to access the internet successfully. When the Lambda function runs, it uses the NAT gateway instead of the gateway VPC endpoint to access Amazon S3.

What can a security engineer do to ensure that the Lambda function uses the gateway VPC endpoint for Amazon S3?

A. Remove the route to the NAT gateway within the route table of the private subnet that the Lambda function uses.

B. Associate the gateway VPC endpoint with the route table of the private subnet that the Lambda function uses.

C. Adjust the gateway VPC endpoint policy to allow access from the Lambda function\\'s network interface address.

D. Configure the Lambda function\\'s security group to allow connections to the S3 network address space.

Correct Answer: B

QUESTION 5

A company has an application that processes personally identifiable information (PII). The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company\\'s security policies require that data is encrypted in transit at all times to avoid the possibility of exposing any PII in plaintext.

Which solutions could a security engineer use to meet these requirements? (Choose two.)

A. Terminate SSL from clients on the existing ALB. Use HTTPS to connect from the ALB to the EC2 instances.

B. Replace the existing ALB with a Network Load Balancer (NLB). On the NLB, configure an SSL listener and TCP passthrough to receive client connections. Terminate HTTPS traffic from the NLB on the EC2 instances.

C. Replace the existing ALB with a Network Load Balancer (NLB). On the NLB, configure TCP passthrough to receive client connections. Terminate SSL from the NLB on the EC2 instances.

D. Configure a Network Load Balancer (NLB) with TCP passthrough to receive client connections. Terminate SSL on the existing ALB.

E. Configure a Network Load Balancer (NLB) with a TLS listener to receive client connections. Configure TCP passthrough on the existing ALB so that the NLB can reach the EC2 instances. Terminate SSL from the ALB on the EC2 instances.

Correct Answer: AB