SCS-C01$^{\text{Q\&As}}$

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

QUESTION 1

A company plans to use custom AMIs to launch Amazon EC2 instances across multiple AWS accounts in a single Region to perform security monitoring and analytics tasks. The EC2 instances are launched in EC2 Auto Scaling groups. To increase the security of the solution, a Security Engineer will manage the lifecycle of the custom AMIs in a centralized account and will encrypt them with a centrally managed AWS KMS CMK. The Security Engineer configured the KMS key policy to allow cross-account access. However, the EC2 instances are still not being properly launched by the EC2 Auto Scaling groups.

Which combination of configuration steps should the Security Engineer take to ensure the EC2 Auto Scaling groups have been granted the proper permissions to execute task?

A. Create a customer-managed CMK in the centralized account. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy. Create an IAM role in all applicable accounts and configure its access policy to allow the use of the centrally managed CMK for cryptographical operations. Configure EC2 Auto Scaling groups within each applicable account to use the created IAM role to launch EC2 instances.

B. Create a customer-managed CMK in the centralized account. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy. Create an IAM role in all applicable accounts and configure its access policy with permissions to create grants for the centrally managed CMK. Use this IAM role to create a grant for the centrally managed CMK with permissions to perform cryptographical operations and with the EC2 Auto Scaling service-linked role defined as the grantee principal.

C. Create a customer-managed CMK or an AWS managed CMK in the centralized account. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy. Use the CMK administrator to create a CMK grant that includes permissions to perform cryptographical operations that define EC2 Auto Scaling service-linked roles from all other accounts as the grantee principal.

D. Create a customer-managed CMK or an AWS managed CMK in the centralized account. Allow other applicable accounts to use that key for cryptographical operations by applying proper cross-account permissions in the key policy. Modify the access policy for the EC2 Auto Scaling roles to perform cryptographical operations against the centrally managed CMK.

Correct Answer: D

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html

QUESTION 2

A company\\'s public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue. the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.

The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.

Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.

B. Configure CloudFront to add a custom: HTTP header to requests that CloudFront sends to the ALB.

C. Configure the ALB to forward only requests that contain the custom HTTP header.

D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.

E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

Correct Answer: BE

QUESTION 3

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

A. Use an AWS Key Management Service (AWS KMS) CMK. Encrypt the data at rest.

B. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.

C. Use a DynamoDB encryption client. Use client-side encryption and sign the table items

D. Use the AWS Encryption SDK. Use client-side encryption and sign the table items.

Correct Answer: A

QUESTION 4

A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manager. A security engineer has installed the Systems Manager Agent on all servers.

The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to them.

The security engineer needs to perform verification steps before Session Manager will work on the servers.

Which combination of steps should the security engineer perform? (Select THREE.)

A. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.

B. Enable the advanced-instances tier in Systems Manager.

C. Create a managed-instance activation for the on-premises servers.

D. Reconfigure the Systems Manager Agent with the activation code and ID.

E. Assign an IAM role to all of the on-premises servers.

F. Initiate an inventory collection with Systems Manager on the on-premises servers

Correct Answer: CEF

QUESTION 5

A company has two VPCs in the us-east-1 Region: vpc-1 and vpe-2. The company recently created an Amazon API Gateway REST API with the endpoint type set to PRIVATE. The company also created a VPC endpoint for the REST API in

vpc-1. Resources in vpc-1 can access the REST API successfully.

The company now wants to give resources in vpc-2 the ability to access the REST API. The company creates a VPC endpoint for the REST API in vpc-2, but the resources in vpc-2 cannot access the REST API.

A security engineer must make the REST API accessible to resources in vpc-2 by creating a solution that provides the minimum access that is necessary.

Which solution will meet these requirements?

A. Set up VPC peering between vpc-1 and vpc-2. Attach an identity-based policy to the resources in vpc-2 to grant access to the REST API.

B. Set up a VPC endpoint of vpc-2 in vpc-1. Attach an identity-based policy to the resources in vpc-2 to grant access to the REST API.

C. Set the API endpoint type to REGIONAL. Attach a resource policy to the REST API to allow access from vpc-2.

D. Keep the API endpoint type as PRIVATE. Attach a resource policy to the REST API to allow access from vpc-2.

Correct Answer: B

[SCS-C01 PDF Dumps](#) [SCS-C01 Study Guide](#) [SCS-C01 Exam Questions](#)