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.leads4pass.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 configured a gateway VPC endpoint in a VPC. Only Amazon EC2 instances that reside in a single subnet in the VPC can use the endpoint. The company has modified the route table for this single subnet to route traffic to Amazon S3 through the gateway VPC endpoint. The VPC provides internet access through an internet gateway.

A security engineer attempts to use instance profile credentials from an EC2 instance to retrieve an object from the S3 bucket, but the attempt fails. The security engineer verifies that the EC2 instance has an IAM instance profile with the correct permissions to access the S3 bucket and to retrieve objects. The security engineer also verifies that the S3 bucket policy is allowing access properly. Additionally, the security engineer verifies that the EC2 instance\\'s security group and the subnet\\'s network ACLs allow the communication.

What else should the security engineer check to determine why the request from the EC2 instance is failing?

A. Verify that the EC2 instance\\'s security group does not have an implicit inbound deny rule for Amazon S3.

B. Verify that the VPC endpoint\\'s security group does not have an explicit inbound deny rule for the EC2 instance.

C. Verify that the internet gateway is allowing traffic to Amazon S3.

D. Verify that the VPC endpoint policy is allowing access to Amazon S3.

Correct Answer: D

QUESTION 2

A company uses Amazon Route 53 to create a public DNS zone for the domain example.com in Account A. The company creates another public DNS zone for the subdomain dev.example.com in Account B. A security engineer creates a wildcard certificate (*.dev.example.com) with DNS validation by using AWS Certificate Manager (ACM). The security engineer validates that the corresponding CNAME records have been created in the zone for dev.example.com in Account

B.

After all these operations are completed, the certificate status is still pending validation.

What should the security engineer do to resolve this issue?

A. Purchase a valid wildcard certificate authority (CA) certificate that supports managed renewal. Import this certificate into ACM in Account B.

B. Add NS records for the subdomain dev.example.com to the Route 53 parent zone example.com in Account A.

C. Use AWS Certificate Manager Private Certificate Authority to create a subordinate certificate authority (CA). Use ACM to generate a private certificate that supports managed renewal.

D. Resend the email message that requests ownership validation of dev.example.com.

Correct Answer: C

QUESTION 3

A security engineer is responsible for providing secure access to AWS resources for thousands of developer in a company\\'s corporate identity provider (idp). The developers access a set of AWS services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when me same set of IAM credentials is used by multiple developer

B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources

C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.

D. Create multiple IAM rotes for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Correct Answer: B

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html

QUESTION 4

A company has been using the AW5 KMS service for managing its keys. They are planning on carrying out housekeeping activities and deleting keys which are no longer in use. What are the ways that can be incorporated to see which keys are in use? Choose 2 answers from the options given below

Please select:

A. Determine the age of the master key

B. See who is assigned permissions to the master key

C. See Cloudtrail for usage of the key

D. Use AWS cloudwatch events for events generated for the key

Correct Answer: BC

The direct ways that can be used to see how the key is being used is to see the current access permissions and cloudtrail logs Option A is invalid because seeing how long ago the key was created would not determine the usage of the key Option D is invalid because Cloudtrail Event is better for seeing for events generated by the key This is also mentioned in the AWS Documentation Examining CMK Permissions to Determine the Scope of Potential Usage Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CM was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key. Examining AWS CloudTrail Logs to Determine Actual Usage AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK\\'s usage history to help you determine whether or not you still need it For more information

on determining the usage of CMK keys, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html The correct answers are: See who is assigned permissions to the master key. See Cloudtrail for usage of the key

QUESTION 5

A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on AWS.

Which combination of AWS services and features will provide protection in this scenario? (Choose three.)

A. Amazon Route 53

B. AWS Certificate Manager (ACM)

C. Amazon S3

D. AWS Shield

E. Elastic Load Balancer

F. Amazon GuardDuty

Correct Answer: ADE

The combination of AWS services and features that provide protection in this scenario are:

A. Amazon Route 53 - This service provides DNS-based routing and can help to mitigate DDoS attacks by using health checks to identify healthy endpoints and automatically routing traffic away from any endpoints that are under attack.

D. AWS Shield - This service provides protection against DDoS attacks at both the network and application layer. It can detect and mitigate attacks in real time, and is available in two tiers: AWS Shield Standard and AWS Shield Advanced.

E. Elastic Load Balancer - ELB provides protection against DDoS attacks by distributing traffic across multiple instances, and by using a range of techniques to filter out malicious traffic. Note: ACM, S3, and GuardDuty are not directly related to mitigating layer 3 and layer 4 DDoS attacks.