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.passapply.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 security team is using Amazon EC2 Image Builder to build a hardened AMI with forensic capabilities. An AWS Key Management Service (AWS KMS) key will encrypt the forensic AMI. EC2 Image Builder successfully installs the required patches and packages in the security team\\'s AWS account. The security team uses a federated IAM role in the same AWS account to sign in to the AWS Management Console and attempts to launch the forensic AMI. The EC2 instance launches and immediately terminates.

What should the security team do to launch the EC2 instance successfully?

A. Update the policy that is associated with the federated IAM role to allow the ec2:DescribeImages action for the forensic AML.

B. Update the policy that is associated with the federated IAM role to allow the ec2:StartInstances action in the security team\\'s AWS account.

C. Update the policy that is associated with the KMS key that is used to encrypt the forensic AMI. Configure the policy to allow the kms:Encrypt and kms:Decrypt actions for the federated IAM role.

D. Update the policy that is associated with the federated IAM role to allow the kms:DescribeKey action for the KMS key that is used to encrypt the forensic AMI.

Correct Answer: C

QUESTION 2

A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.

Which solution meets these criteria?

A. A customer managed CMK that uses customer provided key material

B. A customer managed CMK that uses AWS provided key material

C. An AWS managed CMK

D. Operating system-native encryption that uses GnuPG

Correct Answer: B

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

QUESTION 3

A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company\\'s AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a

suspicious instance until investigation and potential remediation can occur.

Which solution will meet these requirements?

A. Configure GuardDuty to send the event to an Amazon Kinesis data stream. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.

B. Configure GuardDuty to send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy an AWS WAF web ACL. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.

C. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy AWS Network Firewall. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.

D. Enable AWS Security Hub to ingest GuardDuty findings. Configure an Amazon Kinesis data stream as an event destination for Security Hub. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

Correct Answer: B

QUESTION 4

An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.

B. The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.

C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.

D. The version of the Lambda function that was executed was not current.

Correct Answer: A

QUESTION 5

An employee keeps terminating EC2 instances on the production environment. You\\'ve determined the best way to ensure this doesn\\'t happen is to add an extra layer of defense against terminating the instances. What is the best method to ensure the employee does not terminate the production instances? Choose the 2 correct answers from the options below

Please select:

A. Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag.

B. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance call.

C. Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee

D. Modify the IAM policy on the user to require MFA before deleting EC2 instances

Correct Answer: AB

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type -- you can quickly identify a specific resource based on the tags you\\'ve assigned to it. Each tag consists of a key and an optional value, both of which you define Options CandD are incorrect because it will not ensure that the employee cannot terminate the instance. For more information on tagging answer resources please refer to the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Usins_Tags.htmll The correct answers are: Tag the instance with a production-identifying tag and add resource-level permissions to the employe user with an explicit deny on the terminate API call to instances with the production tag.. Tag the instance with a production-identifying tag and modify the employees group to allow only start stop, and reboot API calls and not the terminate instance