TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **SCS-C02**

Title : AWS Certified Security - Specialty

Version : DEMO

1.A business requires a forensic logging solution for hundreds of Docker-based apps running on Amazon EC2.
The solution must analyze logs in real time, provide message replay, and persist logs.
Which Amazon Web Offerings (IAM) services should be employed to satisfy these requirements? (Select two.)
A. Amazon Athena
B. Amazon Kinesis
C. Amazon SQS
D. Amazon Elasticsearch
E. Amazon EMR
Answer: B D

2.A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.
The data includes personally identifiable information (Pll). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.
Which solution will meet this requirement with the MOST operational efficiency?
A. Update the Lambda function to add a TTL S3 flag to S3 objects. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
B. Create an S3 Lifecycle policy to expire objects that are older than 30 days. Update the Lambda function to add the TTL attribute in the DynamoDB table. Enable TTL on the DynamoDB table to expire entires that are older than 30 days based on the TTL attribute.
C. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucket. Update the Lambda function to delete entries that are older than 30 days.
D. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tags. Update the Lambda function to delete entries that are older than 30 days.
Answer: B

3.A company is hosting a static website on Amazon S3 The company has configured an Amazon CloudFront distribution to serve the website contents. The company has associated an IAM WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.
THE company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution
Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.)
A. Select "Restrict Bucket Access" in the origin settings of the CloudFront distribution
B. Create an origin access identity (OAI) for the S3 origin
C. Update the S3 bucket policy to allow s3 GetObject with a condition that the IAM Referer key matches the secret value Deny all other requests
D. Configure the S3 bucket poky so that only the origin access identity (OAI) has read permission for

objects in the bucket
E. Add an origin custom header that has the name Referer to the CloudFront distribution Give the header a secret value.
Answer: A B

4.A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive data-base credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same private subnet. The VPC has a Secrets Manager VPC endpoint.
A security engineer discovers that the secret cannot rotate. The security engineer determines that the VPC endpoint is working as intended. The Amazon Cloud-Watch logs contain the following error: "setSecret: Unable to log into database".
Which solution will resolve this error?
A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the structure that the database requires.
B. Ensure that the security group that is attached to the Lambda function al-lows outbound connections to the EC2 instance. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.
C. Use the Secrets Manager list-secrets command in the AWS CLI to list the secret. Identify the database
credentials. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the secret.
D. Add an internet gateway to the VPC. Create a NAT gateway in a public sub-net. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.
Answer: B
Explanation:
This answer is correct because ensuring that the security groups allow bidirectional communication between the Lambda function and the EC2 instance will resolve the error. The error indicates that the Lambda function cannot connect to the database, which might be due to firewall rules blocking the traffic. By allowing outbound connections from the Lambda function and inbound connections to the EC2 instance, the security engineer can enable the rotation function to access and update the database credentials.

5.A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2 The solution must perform real-time analytics on the togs must support the replay of messages and must persist the logs.
Which IAM services should be used to meet these requirements? (Select TWO)
A. Amazon Athena
B. Amazon Kinesis
C. Amazon SQS
D. Amazon Elasticsearch
E. Amazon EMR

Answer: B D