Latest Version: 22.0

Question: 1

A SysOps Administrator is troubleshooting Amazon EC2 connectivity issues to the internet. The EC2 instance is in a private subnet. Below is the route table that is applied to the subnet of the EC2 instance.
Destination – 10.2.0.0/16
Target – local
Status – Active
Propagated – No
Destination – 0.0.0.0/0
Target – nat-xxxxxxx
Status – Blackhole
Propagated – No
What has caused the connectivity issue?

A. The NAT gateway no longer exists
B. There is no route to the internet gateway.
C. The routes are no longer propagating.
D. There is no route rule with a destination for the internet.

Answer: A

Question: 2

A company has adopted a security policy that requires all customer data to be encrypted at rest. Currently, customer data is stored on a central Amazon EFS file system and accessed by a number of different applications from Amazon EC2 instances.
How can the SysOps Administrator ensure that all customer data stored on the EFS file system meets the new requirement?

A. Update the EFS file system settings to enable server-side encryption using AES-256.
B. Create a new encrypted EFS file system and copy the data from the unencrypted EFS file system to the new encrypted EFS file system.
C. Use AWS CloudHSM to encrypt the files directly before storing them in the EFS file system.
D. Modify the EFS file system mount options to enable Transport Layer Security (TLS) on each of the EC2 instances.

Answer: B

Question: 3

A SysOps Administrator has implemented an Auto Scaling group with a step scaling policy. The Administrator notices that the additional instances have not been included in the aggregated metrics.
Why are the additional instances missing from the aggregated metrics?

A. The warm-up period has not expired
B. The instances are still in the boot process
C. The instances have not been attached to the Auto Scaling group
D. The instances are included in a different set of metrics

Answer: B

Question: 4

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.
What is the SIMPLEST approach the SysOps Administrator can take to ensure S3 buckets in those accounts can never be deleted?

A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being ddeleted.
B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

Answer: B

Question: 5

A company's static website hosted on Amazon S3 was launched recently, and is being used by tens of thousands of users. Subsequently, website users are experiencing 503 service unavailable errors.
Why are these errors occurring?

A. The request rate to Amazon S3 is too high.
B. There is an error with the Amazon RDS database.
C. The requests to Amazon S3 do not have the proper permissions.
D. The users are in different geographical region and Amazon Route 53 is restricting access.

Answer: A