Free Questions for SCS-C01 by ebraindumps

Shared by Medina on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.

The security team is unable to get objects from the S3 bucket

Which factors could cause this issue? (Select THREE.)

Options:

A- The IAM instance profile that is attached to the EC2 instance does not allow the s3 ListBucket action to the S3: bucket in the AWS accounts.

B- The I AM instance profile that is attached to the EC2 instance does not allow the s3 ListParts action to the S3; bucket in the AWS accounts.

C- The KMS key policy that encrypts the object in the S3 bucket does not allow the kms; ListKeys action to the EC2 instance profile ARN.

D- The KMS key policy that encrypts the object in the S3 bucket does not allow the kms Decrypt action to the EC2 instance profile ARN.

E- The security group that is attached to the EC2 instance is missing an outbound rule to the S3 managed prefix list over port 443.

F- The security group that is attached to the EC2 instance is missing an inbound rule from the S3 managed prefix list over port 443.

Answer:

A, D, E

Explanation:

https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html

To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:

The IAM instance profile that is attached to the EC2 instance must allow the s3:GetObject action to the S3 bucket or object in the AWS account. This permission is required to read the object from S3. Option A is incorrect because it specifies the s3:ListBucket action, which is only required to list the objects in the bucket, not to get them.

The KMS key policy that encrypts the object in the S3 bucket must allow the kms:Decrypt action to the EC2 instance profile ARN. This permission is required to decrypt the object using the KMS key. Option D is correct.

The security group that is attached to the EC2 instance must have an outbound rule to the S3 managed prefix list over port 443. This rule is required to allow HTTPS traffic from the EC2 instance to S3 within the AWS infrastructure. Option E is correct. Option B is incorrect because it specifies the s3:ListParts action, which is only required for multipart uploads, not for getting objects. Option C is incorrect because it specifies the kms:ListKeys action, which is not required for getting objects. Option F is incorrect because it specifies an inbound rule from the S3 managed prefix list, which is not required for getting objects. Verified Reference:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html

https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html

Question 2

Question Type: MultipleChoice

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 m 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 learn do lo launch the EC2 instance successfully

Options:

A- Update the policy that is associated with the federated IAM role to allow the ec2. Describelmages action for the forensic AMI.

B- Update the policy that is associated with the federated IAM role to allow the ec2 Start Instances action m 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.

Answer:

C

Explanation:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-internal

Question 3

Question Type: MultipleChoice

A company has a relational database workload that runs on Amazon Aurora MySQL. According to new compliance standards the company must rotate all database credentials every 30 days. The company needs a solution that maximizes security and minimizes development effort.

Which solution will meet these requirements?

Options:

A- Store the database credentials in AWS Secrets Manager. Configure automatic credential rotation tor every 30 days.

B- Store the database credentials in AWS Systems Manager Parameter Store. Create an AWS Lambda function to rotate the credentials every 30 days.

C- Store the database credentials in an environment file or in a configuration file. Modify the credentials every 30 days.

D- Store the database credentials in an environment file or in a configuration file. Create an AWS Lambda function to rotate the credentials every 30 days.

Answer:

A

Explanation:

To rotate database credentials every 30 days, the most secure and efficient solution is to store the database credentials in AWS Secrets Manager and configure automatic credential rotation for every 30 days. Secrets Manager can handle the rotation of the credentials in both the secret and the database, and it can use AWS KMS to encrypt the credentials. Option B is incorrect because it requires creating a custom Lambda function to rotate the credentials, which is more effort than using Secrets Manager. Option C is incorrect because it stores the database credentials in an environment file or a configuration file, which is less secure than using Secrets Manager. Option D

is incorrect because it combines the drawbacks of option B and option C. Verified Reference:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-other.html

Question 4

Question Type: MultipleChoice

A company wants to configure DNS Security Extensions (DNSSEC) for the company's primary domain. The company registers the domain with Amazon Route 53. The company hosts the domain on Amazon EC2 instances by using BIND.

What is the MOST operationally efficient solution that meets this requirement?

Options:

A- Set the dnssec-enable option to yes in the BIND configuration. Create a zone-signing key (ZSK) and a key-signing key (KSK) Restart the BIND service.

B- Migrate the zone to Route 53 with DNSSEC signing enabled. Create a zone-signing key (ZSK) and a key-signing key (KSK) that are based on an AWS. Key Management Service (AWS KMS) customer managed key.

C- Set the dnssec-enable option to yes in the BIND configuration. Create a zone-signing key (ZSK) and a key-signing key (KSK). Run the dnssec-signzone command to generate a delegation signer (DS) record Use AWS. Key Management Service (AWS KMS) to secure the keys.

D- Migrate the zone to Route 53 with DNSSEC signing enabled. Create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed key. Add a delegation signer (DS) record to the parent zone.

Answer:

D

Explanation:

To configure DNSSEC for a domain registered with Route 53, the most operationally efficient solution is to migrate the zone to Route 53 with DNSSEC signing enabled, create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed key, and add a delegation signer (DS) record to the parent zone. This way, Route 53 handles the zone-signing key (ZSK) and the signing of the records in the hosted zone, and the customer only needs to manage the KSK in AWS KMS and provide the DS record to the domain registrar. Option A is incorrect because it does not involve migrating the zone to Route 53, which would simplify the DNSSEC configuration. Option B is incorrect because it creates both a ZSK and a KSK based on AWS KMS customer managed keys, which is unnecessary and less efficient than letting Route 53 manage the ZSK. Option C is incorrect because it does not involve migrating the zone to Route 53, and it requires running the dnssec-signzone command manually, which is less efficient than letting Route 53 sign the zone automatically. Verified Reference:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html

https://aws.amazon.com/about-aws/whats-new/2020/12/announcing-amazon-route-53-support-dnssec/

Question 5

Question Type: MultipleChoice

A developer has created an AWS Lambda function in a company's development account. The Lambda function requires the use of an AWS Key Management Service (AWS KMS) customer managed key that exists in a security account that the company's security team controls. The developer obtains the ARN of the KMS key from a previous Lambda function in the development account. The previous Lambda function had been working properly with the KMS key.

When the developer uses the ARN and tests the new Lambda function an error message states that access is denied to the KMS key in the security account. The developer tests the previous Lambda function that uses the same KMS key and discovers that the previous Lambda function still can encrypt data as expected.

A security engineer must resolve the problem so that the new Lambda function in the development account can use the KMS key from the security account.

Which combination of steps should the security engineer take to meet these requirements? (Select TWO.)

Options:

A- In the security account configure an IAM role for the new Lambda function. Attach an IAM policy that allows access to the KMS key in

the security account.

B- In the development account configure an IAM role for the new Lambda function. Attach a key policy that allows access to the KMS key in the security account.

C- In the development account configure an IAM role for the new Lambda function. Attach an IAM policy that allows access to the KMS key in the security account.

D- Configure a key policy for the KMS key m the security account to allow access to the IAM role of the new Lambda function in the security account.

E- Configure a key policy for the KMS key in the security account to allow access to the IAM role of the new Lambda function in the development account.

Answer:

C, E

Explanation:

To allow cross-account access to a KMS key, the key policy of the KMS key must grant permission to the external account or principal, and the IAM policy of the external account or principal must delegate the key policy permission. In this case, the new Lambda function in the development account needs to use the KMS key in the security account, so the key policy of the KMS key must allow access to the IAM role of the new Lambda function in the development account (option E), and the IAM role of the new Lambda function in the development account must have an IAM policy that allows access to the KMS key in the security account (option C). Option A is incorrect because it creates an IAM role for the new Lambda function in the security account, not in the development account. Option B is incorrect because it attaches a key policy to an IAM role, which is not valid. Option D is incorrect because it allows access to the IAM

role of the new Lambda function in the security account, not in the development account. Verified Reference:

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

https://docs.aws.amazon.com/autoscaling/ec2/userguide/key-policy-requirements-EBS-encryption.html

Question 6

Question Type: MultipleChoice

A company wants to prevent SSH access through the use of SSH key pairs for any Amazon Linux 2 Amazon EC2 instances in its AWS account. However, a system administrator occasionally will need to access these EC2 instances through SSH in an emergency. For auditing purposes, the company needs to record any commands that a user runs in an EC2 instance.

What should a security engineer do to configure access to these EC2 instances to meet these requirements?

Options:

A- Use the EC2 serial console Configure the EC2 serial console to save all commands that are entered to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows the EC2 serial console to access Amazon S3. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use the EC2 serial console.

B- Use EC2 Instance Connect Configure EC2 Instance Connect to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instances with an IAM role that allows the EC2 instances to access CloudWatch Logs Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use EC2 Instance Connect.

C- Use an EC2 key pair with an EC2 instance that needs SSH access Access the EC2 instance with this key pair by using SSH. Configure the EC2 instance to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instance with an IAM role that allows the EC2 instance to access Amazon S3 and CloudWatch Logs.

D- Use AWS Systems Manager Session Manager Configure Session Manager to save all commands that are entered in a session to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows Systems Manager to manage the EC2 instances. Configure an IAM account for the system administrator Provide an IAM policy that allows the IAM account to use Session Manager.

Answer:

D

Explanation:

Open the AWS Systems Manager console at https://console.aws.amazon.com/systems-manager/. In the navigation pane, choose Session Manager. Choose the Preferences tab, and then choose Edit. Select the check box next to Enable under S3 logging. (Recommended) Select the check box next to Allow only encrypted S3 buckets. With this option turned on, log data is encrypted using the server-side encryption key specified for the bucket. If you don't want to encrypt the log data that is sent to Amazon S3, clear the check box. You must also clear the check box if encryption isn't allowed on the S3 bucket.

Question 7

Question Type: MultipleChoice

A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1. Region Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at test. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.

The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.

After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.

Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

Options:

A- Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.

B- Grant the IAM role the kms. Encrypt permission for the key in us-east-1 that encrypts source objects.

C- Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.

D- Grant the IAM role the kms. Decrypt permission for the key in us-east-1 that encrypts source objects.

E- Change the key policy of the key in us-east-1 to grant the kms. Decrypt permission to the security engineer's IAM account.

F- Grant the IAM role the kms Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

Answer:

B, F

Explanation:

To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects. This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role.

This solution will remediate the issue of encrypted objects not being replicated to the destination bucket.

The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).

Verified Reference:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html