AWS Certified Security - Specialty

Version: V23.01 - Demo

1 A company's on-premises networks are connected to VPCs using an IAM Direct Connect gateway. The company's on-premises application needs to stream data using an existing Amazon Kinesis Data Firehose delivery stream. The company's security policy requires that data be encrypted in transit using a private network.
How should the company meet these requirements?

A. Create a VPC endpoint tor Kinesis Data Firehose. Configure the application to connect to the VPC endpoint.

B. Configure an IAM policy to restrict access to Kinesis Data Firehose using a source IP condition.
Configure the application to connect to the existing Firehose delivery stream.

C. Create a new TLS certificate in IAM Certificate Manager (ACM). Create a public-facing Network Load Balancer (NLB) and select the newly created TLS certificate. Configure the NLB to forward all traffic to Kinesis Data Firehose. Configure the application to connect to the NLB.

D. Peer the on-premises network with the Kinesis Data Firehose VPC using Direct Connect. Configure the application to connect to the existing Firehose delivery stream.
Answer: A

2 You have a 2 tier application hosted in IAM. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.
Please select:

A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0

B. db-345 - Allow port 1433 from wg-123

C. wg-123 - Allow port 1433 from wg-123

D. db-345 -Allow ports 1433 from 0.0.0.0/0
Answer: A B

3 A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The

company also must rotate the credentials automatically on a regular basis.
Which solution meets these requirements?

A. Use IAM Systems Manager Parameter Store to store the database credentials. Configure automatic rotation of the credentials.

B. Use IAM Secrets Manager to store the database credentials. Configure automat* rotation of the credentials.

C. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.

D. Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the credentials on a scheduled basis

Answer: A

4 Your IT Security team has advised to carry out a penetration test on the resources in their company's IAM Account. This is as part of their capability to analyze the security of the infrastructure. What should be done first in this regard?
Please select:

A. Turn on Cloud trail and carry out the penetration test

B. Turn on VPC Flow Logs and carry out the penetration test

C. Submit a request to IAM Support

D. Use a custom IAM Marketplace solution for conducting the penetration test

Answer: C

5 You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.
Please select:

A. IAM KMS

B. IAM Customer Keys

C. IAM managed keys

D. IAM Cloud HSM

Answer: A D

6 A website currently runs on Amazon EC2 with mostly static content on the site. Recently, the site was subjected to a DDoS attack, and a Security Engineer was tasked with redesigning the edge security to help mitigate this risk in the future What are some ways the Engineer could achieve this? (Select THREE)

A. Use IAM X-Ray to inspect the traffic going 10 the EC2 instances

B. Move the state content to Amazon S3 and font this with an Amazon CloudFront distribution

C. Change the security group configuration to block the source of the attack traffic

D. Use IAM WAF security rules to inspect the inbound traffic

E. Use Amazon inspector assessment templates to inspect the inbound traffic

F. Use Amazon Route 53 to distribute traffic

Answer: B D F

7 A corporation is preparing to acquire several companies. A Security Engineer must design a solution to ensure that newly acquired IAM accounts follow the corporation's security best practices. The solution should monitor each Amazon S3 bucket for unrestricted public write access and use IAM managed services.

What should the Security Engineer do to meet these requirements?

A. Configure Amazon Macie to continuously check the configuration of all S3 buckets.

B. Enable IAM Config to check the configuration of each S3 bucket.

C. Set up IAM Systems Manager to monitor S3 bucket policies for public write access.

D. Configure an Amazon EC2 instance to have an IAM role and a cron job that checks the status of all S3 buckets.

Answer: C

8 A company is outsourcing its operational support 1o an external company. The company's security officer must implement an access solution fen delegating operational support that minimizes overhead.

Which approach should the security officer take to meet these requirements?

A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider

B. Federate IAM identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions

C. Create an IAM group for me external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the eternal company.

D. Use IAM SSO with the external company's identity provider. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

9 An Amazon EC2 instance is denied access to a newly created IAM KMS CMK used for decrypt actions. The environment has the following configuration:

* The instance is allowed the kms:Decrypt action in its IAM role for all resources
* The IAM KMS CMK status is set to enabled
* The instance can communicate with the KMS API using a configured VPC endpoint What is causing the issue?

A. The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role

B. The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN

C. The kms:Encrypt permission is missing from the EC2 IAM role

D. The KMS CMK key policy that enables IAM user permissions is missing

Answer: D

10 Your company has just started using IAM and created an IAM account. They are aware of the potential issues when root access is enabled. How can they best safeguard the account when it comes to root access? Choose 2 answers fro the options given below Please select:

A. Delete the root access account

B. Create an Admin IAM user with the necessary permissions

C. Change the password for the root account.

D. Delete the root access keys

Answer: B D