Free Questions for SCS-C01 by vceexamstest

Shared by Franks on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.

Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.

The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.

How will the security engineer be able to comply with these requirements?

Options:

A- Remove the existing NAT gateway. Create a new NAT gateway that only the application server subnets can use.

B- Configure the DB instances inbound network ACL to deny traffic from the security group ID of the NAT gateway.

C- Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.

D- Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

Answer:

C

Explanation:

Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

Question 2

Question Type: MultipleChoice

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 (AWS) services should be employed to satisfy these requirements? (Select two.)

Options:

A- Amazon Athena

B- Amazon Kinesis

C- Amazon SQS

D- Amazon Elasticsearch

E- Amazon EMR

Answer:

B, D

Question 3

Question Type: MultipleChoice

A company has two teams, and each team needs to access its respective Amazon S3 buckets. The company anticipates adding more teams that also will have their own S3 buckets. When the company adds these teams, team members will need the ability to be assigned to multiple teams. Team members also will need the ability to change teams. Additional S3 buckets can be created or deleted.

An 1AM administrator must design a solution to accomplish these goals. The solution also must be scalable and must require the least possible operational overhead.

Which solution meets these requirements?

Options:

A- Add users to groups that represent the teams. Create a policy for each team that allows the team to access its respective S3 buckets only. Attach the policy to the corresponding group.

B- Create an 1AM role for each team. Create a policy for each team that allows the team to access its respective S3 buckets only. Attach the policy to the corresponding role.

C- Create 1AM roles that are labeled with an access tag value of a team. Create one policy that allows dynamic access to S3 buckets with the same tag. Attach the policy to the 1AM roles. Tag the S3 buckets accordingly.

D- Implement a role-based access control (RBAC) authorization model. Create the corresponding policies, and attach them to the 1AM users.

Answer:

A

Question 4

Question Type: **MultipleChoice**

A security engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the security engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy, the employee still receives an access denied message.

What is the likely cause of this access denial?

A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.

The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.

Which combination of actions should the security engineer recommend to meet these requirements? (Select THREE.)

Options:

A- Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.

B- Place the DB instance in a public subnet.

C- Place the DB instance in a private subnet.

D- Configure the Auto Scaling group to place the EC2 instances in a public subnet.

E- Configure the Auto Scaling group to place the EC2 instances in a private subnet.

F- Deploy the ALB in a private subnet.

Answer:

A, C, E

Question 5

Question Type: **MultipleChoice**

A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.

Which factors could cause the health check failures? (Select THREE.)

Options:

A- The target instance's security group does not allow traffic from the NLB.

B- The target instance's security group is not attached to the NLB.

C- The NLB's security group is not attached to the target instance.

D- The target instance's subnet network ACL does not allow traffic from the NLB.

E- The target instance's security group is not using IP addresses to allow traffic from the NLB.

F- The target network ACL is not attached to the NLB.

Answer:

A, C, D

Question 6

Question Type: MultipleChoice

A company's application team needs to host a MySQL database on AWS. According to the company's security policy, all data that is stored on AWS must be encrypted at rest. In addition, all cryptographic material must be compliant with FIPS 140-2 Level 3 validation.

The application team needs a solution that satisfies the company's security requirements and minimizes operational overhead.

Which solution will meet these requirements?

Options:

A- Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an AWS Key Management Service (AWS KMS) custom key store that is backed by AWS CloudHSM for key management.

B- Host the database on Amazon RDS. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use an AWS managed CMK in AWS Key Management Service (AWS KMS) for key management.

D- Host the database on an Amazon EC2 instance. Use Amazon Elastic Block Store (Amazon EBS) for encryption. Use a customer managed CMK in AWS Key Management Service (AWS KMS) for key management.

E- Host the database on an Amazon EC2 instance. Use Transparent Data Encryption (TDE) for encryption and key management.

Answer:

B

Question 7

Question Type: MultipleChoice

Options:

A- The 1AM 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 1AM 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 n the S3 bucket does not allow the kms:Decrypt a:: r to re 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, C, D

Question 8

Question Type: MultipleChoice

A company is hosting multiple applications within a single VPC in its AWS account. The applications are running behind an Application Load Balancer that is associated with an AWS WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.

A security engineer needs to deny access from the offending IP addresses.

Which solution will meet these requirements?

Options:

A- Modify the AWS WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.

B- Add a rule to all security groups to deny the incoming requests from the IP address range.

C- Modify the AWS WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.

D- Configure the AWS WAF web ACL with regex match conditions. Specify a pattern set to deny the incoming requests based on the match condition

Answer:

A

Explanation:

Note that the IP is known and the question wants us to deny access from that particular address and so we can use IP set match policy of WAF to block access.

Question 9

Question Type: **MultipleChoice**

A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.

During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.

Which combination of options can the company use to meet these requirements? (Select TWO.)

Options:

A- Create a snapshot of the DB instance. Copy the snapshot to a new snapshot, and enable encryption for the copy process. Use the new snapshot to restore the DB instance.

B- Modify the configuration of the DB instance by enabling encryption. Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.

C- Use AWS Key Management Service (AWS KMS) to create a new default AWS managed awa/rds key. Select this key as the encryption key for operations with Amazon RDS.

D- Use AWS Key Management Service (AWS KMS] to create a new CMK. Select this key as the encryption key for operations with Amazon RDS.

E- Create a snapshot of the DB instance. Enable encryption on the snapshoVUse the snapshot to restore the DB instance.

Answer:

C, E