Free Questions for SAA-C03 by ebraindumps

Shared by Lang on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC

Options:

A) The application requires access to a database in VPC B. Both VPCs are in the same AWS account.
Which solution will provide the required access MOST securely?

A) Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.

B) Configure a VPC peering connection between VPC A and VPC B.

C) Make the DB instance publicly accessible. Assign a public IP address to the DB instance.

D) Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Answer:

B

Explanation:

A VPC peering connection is a networking connection between two VPCs that enables users to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network.A VPC peering connection can be created between VPCs in the same or different AWS accounts and Regions1. By configuring a VPC peering connection between VPC A and VPC B, the solution can provide the required access most securely.

A) Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and relying on a single IP address for access control2.

C) Make the DB instance publicly accessible. Assign a public IP address to the DB instance.This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and allowing any source to connect to it2.

D) Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.This solution will not provide the required access most securely, as it involves creating an additional resource and configuring a proxy server that may introduce latency and complexity3.

Reference URL: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Question 2

Question Type: MultipleChoice

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

Image not found or type unknown

A Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.

Options:

B) Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).

C) Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are
permitted any other Amazon EC2 action.

D) Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Answer:

D

Explanation:

This answer is correct because it reflects the effect of the IAM policy on the group members. The policy has two statements: one with an Allow effect and one with a Deny effect. The Allow statement grants permission to perform any EC2 action on any resource within the us-east-1 Region. The Deny statement overrides the Allow statement and denies permission to perform the ec2:StopInstances and ec2:TerminateInstances actions on any resource within the us-east-1 Region, unless the group member is logged in with MF

A) Therefore, the group members can perform any EC2 action except stopping or terminating instances in the us-east-1 Region, unless they use MFA.

Question 3

Question Type: **MultipleChoice**

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

Options:

A) Set up a VPC peering connection between VPC-A and VPC-B.

B) Set up VPC gateway endpoints for the EC2 instance running in VPC-B.

C) Attach a virtual private gateway to VPC-B and set up routing from VPC-A.

D) Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Answer:

A

Explanation:

.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.
https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Question 4

Question Type: MultipleChoice

An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account.

Which solution will provide the required access MOST securely?

Options:

A) Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.

B) Configure a VPC peering connection between VPC A and VPC B.

C) Make the DB instance publicly accessible. Assign a public IP address to the DB instance.

D) Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Answer:

B

Explanation:

.

A VPC peering connection is a networking connection between two VPCs that enables users to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network.A VPC peering connection can be created between VPCs in the same or different AWS accounts and Regions1. By configuring a VPC peering

connection between VPC A and VPC B, the solution can provide the required access most securely.

A) Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and relying on a single IP address for access control2.

C) Make the DB instance publicly accessible. Assign a public IP address to the DB instance.This solution will not provide the required access most securely, as it involves exposing the DB instance to the public internet and allowing any source to connect to it2.

D) Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.This solution will not provide the required access most securely, as it involves creating an additional resource and configuring a proxy server that may introduce latency and complexity3.

Reference URL: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Question 5

Question Type: **MultipleChoice**

A developer has an appfccabon that uses an AWS Lambda function to upload fies to Amazon S3 and needs the required permissions lo perform the task The developer already has an 1AM user with valid 1AM credentials required for Amazon S3

What should a solutions architect do to grant the permissions?

Options:

A) Add required 1AM permissions in the resource policy of the Lambda function

B) Create a signed request using the existing 1AM credentials n the Lambda function

C) Create a new 1AM user and use the existing 1AM credentials in the Lambda function.

D) Create an 1AM execution role with the required permissions and attach the 1AM rote to the Lambda runcton

Answer:

D

Question 6

Question Type: MultipleChoice

A company is building a new dynamic ordering website. The company wants 10 minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as qutddy as possible to meet changes in user demand.

Which solution will meet ftese requirements?

Options:

A) Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon DynamoDB with on-demand capacity for the database Configure Amazon CtoudFront to deliver the website content

B) Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon Aurora with Aurora Auto Scaling for the database Configure Amazon CloudFront to deliver the website content

C) Host al the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 Instances Use an Application Load Balancer to distribute traffic Use Amazon DynamoDB with provisioned write capacity for the database

D) Host at the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 instances Use an Application Load Balancer to distribute traffic Use Amazon Aurora with Aurora Auto Scaling for the database

Answer:

A

Question 7

Question Type: MultipleChoice

A company runs a containerised application on a Kubernetes cluster m an on premises data center The company is using a MongoOB drtabii tor dan atanige The company wants to migrate some of these environments to AWS but no code changes or deployment method changes ate possible at this time The company needs a solution mat minimizes operational overhead

Which solution meets these requirements?

Options:

A) Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoOB on EC2 for data storage

B) Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB tor data storage

C) Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage

D) Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS fargate for compute and Amazon DocumentDB (with MongoOB compatfciMy) for data storage

Answer:

D

Explanation:

Amazon DocumentDB (with MongoDB compatibility) is a fast, reliable, and fully managed database service. Amazon DocumentDB makes it easy to set up, operate, and scale MongoDB-compatible databases in the cloud. With Amazon DocumentDB, you can run the same application code and use the same drivers and tools that you use with MongoDB.

https://docs.aws.amazon.com/documentdb/latest/developerguide/what-is.html

Question 8

Question Type: MultipleChoice

A company runs an applcalion on a large Heel of Amazon EC2 ratances. The application leads and write entries into an Amazon DynamoDB (able The size of the DynamoDB table continuously grows but the application needs only data from the last 30 days. The company needs a solution that mmmizes cost and development effort.

Which solution meets these requirements?

Options:

A) Use an AWS CloudFomiahon template to deploy the complete solution Redeploy the CloudFormation stack every 30 days and delete the original stack

B) Use an EC2 Instance that runs a monitonng application from AWS Marketplace Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table Use a scnpt that runs on the EC2 instance to delele items that have a timestamp that is older than 30 days

C) Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table Configure the Lambda function to delete items in the table that are older than 30 days

D) Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the (able Configure DynamoDB to use the attribute as (he TTL attribute

Answer:

D

Explanation:

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs.

TTL is useful if you store items that lose relevance after a specific time. The following are example TTL use cases:

Remove user or sensor data after one year of inactivity in an application.

Archive expired items to an Amazon S3 data lake via Amazon DynamoDB Streams and AWS Lambda.

Retain sensitive data for a certain amount of time according to contractual or regulatory obligations.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html