CertSharks

Amazon AWS Certified Solutions Architect - Associate (SAA-C03)

Version: V23.01 - Demo

1 A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

A. Set up a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.

B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.

C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.

D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Answer: B

2 A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

A. Create an IAM role that includes permissions to access Lake Formation tables.

B. Create data filters to implement row-level security and cell-level security.

C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests re data.

D. Create an AWS Lambda function that periodically Queries and removes sensitive information from Lake Formation tables.

Answer: B

3 A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.

B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.

C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.

D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Answer: A

4 A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.
The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.
Which solution will meet these requirements MOST cost-effectively?

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.

D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Answer: A

5 A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days Which storage solution is MOST costeffective?

A. Create an S3 bucket lifecycle policy to move Mm from S3 Standard to S3 Glacier
30 days from object creation Delete the Tiles 4 years after object creation

B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA] 30 days from object creation. Delete the fees 4 years after object creation

C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard
-lA) 30 from object creation. Delete the ties 4 years after object creation

D. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation Move the files to S3 Glacier 4 years after object carton.

Answer: B

6 A company is preparing to store confidential data in Amazon S3 For compliance reasons the data must be encrypted at rest Encryption key usage must be logged tor auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and the MOST operationally efferent?

A. Server-side encryption with customer-provided keys (SSE-C)

B. Server-side encryption with Amazon S3 managed keys (SSE-S3)

C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation

D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automate rotation.

Answer: D

7 A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located.

Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy lo the S3 bucket to only allow the EC2 instance's IAM role for access.

C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
D. Use the AWS provided, publicly available ip-ranges.json tile to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
Answer: A

8 A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.
What should the solutions architect do to enable Internet access for the private subnets?
A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.
Answer: A

9 A company has implemented a self-managed DNS service on AWS. The solution consists of the following:
* Amazon EC2 instances in different AWS Regions
* Endpomts of a standard accelerator m AWS Global Accelerator
The company wants to protect the solution against DDoS attacks What should a solutions architect do to meet this requirement?
A. Subscribe to AWS Shield Advanced Add the accelerator as a resource to protect
B. Subscribe to AWS Shield Advanced Add the EC2 instances as resources to protect
C. Create an AWS WAF web ACL that includes a rate-based rule Associate the web ACL with the accelerator

D. Create an AWS WAF web ACL that includes a rate-based rule Associate the web ACL with the EC2 instances

Answer: A

10 A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All
non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

A. Configure the Lambda function to run in the VPC with the appropriate security group.

B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.

C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.

D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Answer: A