Question 1 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

A start-up firm has created a cloud storage application that gives users the ability to store any amount of personal data & share them with their connections. For this, they are using Amazon S3 buckets to store user data. The firm has used Amazon S3 multipart upload to upload large objects in parts. During the last quarter, the finance team has observed a surge in storage costs for the S3 bucket. On further checking, the firm observed that many 100 GB files are uploaded by users & are in a partially completed state.

As an AWS consultant, the IT Team requests you prevent this from happening again. Which of the following actions can be taken to meet this requirement cost-effectively with the least effort?

- (●) A. Create an S3 lifecycle Configuration to abort incomplete multipart uploads.
- ( ) B. Manually delete incomplete multipart uploads from the S3 bucket.
- ( ) C. Use Cron tool to identify incomplete uploads & delete those files.
- ( ) D. No action is required. All Incomplete uploads are automatically deleted every three months by Amazon S3.

Question 2 of 65

Exit Quiz

Domain: Design High-Performing Architectures

Your Operations department is using an incident-based application hosted on a set of EC2 Instances. These instances are placed behind an Auto Scaling Group to ensure that the right number of instances are in place to support the application. The Operations department has expressed dissatisfaction concerning poor application performance every day at 9:00 AM. However, it is also noted that the system performance returns to optimal at 9:45 AM.

What could be done to fix this issue?

- A. Create another Dynamic Scaling Policy to ensure that the scaling happens at 9:00 AM.
- B. Add another Auto Scaling group to support the current one.
- C. Change the Cool Down Timers for the existing Auto Scaling Group.
- D. Add a Scheduled Scaling Policy at 8:30 AM.

Question 3 of 65

Exit Quiz

Domain: Design Secure Architectures

You have created an AWS Lambda function that will write data to a DynamoDB table. Which of the following must be in place to ensure that the Lambda function can interact with the DynamoDB table?

- A. Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges.
- B. Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.
- C. Ensure the Access keys are embedded in the AWS Lambda function.
- D. Ensure the IAM user password is embedded in the AWS Lambda function.

show Answer

Domain: Design Cost-Optimized Architectures

A Media firm is saving all its old videos in S3 Glacier Deep Archive. Due to the shortage of new video footage, the channel has decided to reuse all these old videos. Since these are old videos, the channel is not sure of their popularity & response from users. Channel Head wants to make sure that these huge size files do not shoot up their budget. For this, as an AWS consultant, you advise them to use the S3 intelligent storage class. The Operations Team is concerned about moving these files to the S3 Intelligent-Tiering storage class. Which of the following actions can be taken to move objects in Amazon S3 Glacier Deep Archive to the S3 Intelligent-Tiering storage class?

- A. Use Amazon S3 Console to copy these objects from S3 Glacier Deep Archive to the required S3 Intelligent-Tiering storage class.
- B. Use Amazon S3 Glacier Console to restore objects from S3 Glacier Deep Archive & then copy these objects to the required S3 Intelligent-Tiering storage class.
- C. Use Amazon S3 console to restore objects from S3 Glacier Deep Archive & then copy these objects to the required S3 Intelligent-Tiering storage class.
- D. Use the Amazon S3 Glacier console to copy these objects to the required S3 Intelligent-Tiering storage class.

Question 5 of 65

Exit Quiz

Domain: Design Secure Architectures

You have a cluster of Windows instances joined to an AWS Managed Active Directory. You want to have a shared storage for all these instances and control this storage access with the Managed Active Directory. Which of the following services allows you to achieve this?

- A. Amazon FSx for Lustre
- B. Amazon FSx for Windows File Server
- C. Amazon EFS
- D. Use S3 and AD Connector

show Answer

Question 6 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

You are part of the IT team of an insurance company. You have 4 M5.large EC2 instances used to compute some data of your core services. The amount of usage of these instances has been very consistent. So you predict that it will not increase in the next two or three years. However, your CFO is asking if there is a way to reduce costs in the EC2 instances. What do you suggest to get the maximum cost reduction?

A. Use a Compute Savings Plan.

B. Use an EC2 instance Savings Plan.

C. Use a Convertible Reserved Instance.

D. Use a Dedicated Instance.

Question 7 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

You are building an automated transcription service where Amazon EC2 worker instances process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. Customers fetch the text files frequently. You do not know about the storage capacity requirements. Which storage option would be both cost-efficient and highly available in this situation?

A. Multiple Amazon EBS Volume with snapshots

B. A single Amazon Glacier Vault

C. A single Amazon S3 bucket

D. Multiple instance stores

Question 8 of 65

Exit Quiz

Domain: Design High-Performing Architectures

A customer has an instance hosted in the public subnet of the default VPC. The subnet has the default settings for the Network Access Control List. An IT Administrator needs to be provided SSH access to the underlying instance. How could this be accomplished?

- A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation.
- B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation.
- C. Ensure that the Security group allows Inbound SSH traffic from the IT Administrator's Workstation.
- D. Ensure that the Security group allows Outbound SSH traffic from the IT Administrator's Workstation.

Question 9 of 65

Exit Quiz

Domain: Design Secure Architectures

Your Organization is planning to move its on-premise databases to the AWS Cloud. You have been selected to migrate the main production database, and there are some requirements. The production database should remain active during the migration. You need to monitor the progress of the migration. The database is an SQL Server Database. You need to find an easy way to convert the actual schemas to MySQL schemas. What services could help to achieve this? (Select two)

- [ ] A. AWS DataSync.
- [ ] B. AWS Server Migration Service.
- [x] C. AWS Database Migration Service.
- [x] D. AWS Migration Hub.
- [ ] E. AWS Server Migration Service Connector.

Question 10 of 65

Exit Quiz

Domain: Design High-Performing Architectures

You are deploying an application to track the GPS coordinates of delivery trucks in the United States. Coordinates are transmitted from each delivery truck once every three seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple consumers. Which of the following services would you use to implement data ingestion?

- A. Amazon Kinesis
- B. AWS Data Pipeline
- C. Amazon Elastic Transcoder
- D. Amazon Simple Queue Service

Question 11 of 65

Exit Quiz

Domain: Design High-Performing Architectures

With its own Active Directory, your company authenticates users for different applications. You have been assigned the task of consolidating and migrating services to the cloud and using the same credentials if possible. What would you recommend?

- A. Use AWS Directory Service that allows users to sign in with their existing corporate credentials.
- B. Create two Active Directories – one for the cloud and one for on-premises – reducing username/password combinations to two.
- C. Require users to use third-party identity providers to log-in for all services.
- D. Build out Active Directory on EC2 instances to gain more control over user profiles.

Question 12 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

A company is planning to use the AWS Redshift service. The Redshift service and data on it would be used continuously for the next 3 years as per the current business plan. What would be the most cost-effective solution in this scenario?

A. Consider using On-demand instances for the Redshift Cluster.

B. Enable Automated backup.

C. Consider using Reserved Instances for the Redshift Cluster.

D. Consider not using a cluster for the Redshift nodes.

Question 13 of 65

Exit Quiz

Domain: Design High-Performing Architectures

A company has recently started using AWS Cloud services and needs to transfer a large set of data online from on-prem Windows servers to AWS Storage Services S3, EFS, and FSx. The data can be transferred in opposite directions periodically and should be incremental based on schedules.
How would a Solution Architect design this solution?

- A. Use Snowball devices to transfer data to S3, EFS and FSx.
- B. Use AWS DataSync service to transfer data to AWS Services.
- C. AWS Database Migration Service to transfer data to AWS services.
- D. Use AWS S3 Transfer acceleration to transfer a large set of data.

Question 14 of 65

Exit Quiz

Domain: Design Secure Architectures

You have a PHP application deployed in an Auto Scaling group. In production, you want to use AWS WAF to block requests associated with exploiting vulnerabilities specific to the PHP use, including injection of unsafe PHP functions. Which method is appropriate?

- A. Add the AWS managed PHP application rule to AWS Shield.
- B. Add the AWS managed PHP application rule in the web ACL of AWS WAF.
- C. Add a PHP protection rule from AWS Marketplace to the WAF web ACL.
- D. Override the PHP rule's actions under the 'ExcludedRules' specification inside a rule group of a web ACL.

Question 15 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

A large amount of structured data is stored in Amazon S3 using the JSON format. You need to use a service to analyze the S3 data directly with standard SQL. In the meantime, the data should be easily visualized through data dashboards. Which of the following services is the most appropriate?

- A. Amazon Athena and Amazon QuickSight.
- B. AWS Glue and Amazon Athena.
- C. AWS Glue and Amazon QuickSight.
- D. Amazon Kinesis Data Stream and Amazon QuickSight.

Question 16 of 65

Exit Quiz

Domain: Design Secure Architectures

An AWS Organization has the below hierarchy of Organizational Units (OUs):

Root -> Project_OU -> Dev_OU

The Root is attached to the default Service Control Policy (SCP).

Project_OU is attached to an SCP that prevents users from deleting VPC Flow Logs.

Dev_OU has an SCP that allows the action of "ec2: DeleteFlowLogs".

Are the IAM users/roles in Dev_OU AWS accounts allowed to delete VPC Flow Logs?

A. It is permitted because the SCP in Dev_OU allows it.

B. It is allowed because the Root has the default SCP that allows all actions.

C. It is not allowed as the SCP in Project_OU restricts the action.

D. It is not allowed as the default SCP in Root denies the action.

Question 17 of 65

Exit Quiz

Domain: Design Secure Architectures

One AWS Organization owns several AWS accounts. Recently, due to a change of company organizations, one member account needs to be moved from this AWS Organization to another one. How can you achieve this?

- A. In the AWS console, drag and drop this account from one Organization to another.
- B. In the AWS console, select the member account and migrate it to the destination AWS Organization.
- C. Delete the old AWS Organization. Send an invite from the new Organization and accept the invite for the member account.
- D. Remove the member account from the old Organization. Send an invite from the new Organization to the member account and accept the invite.

Question 18 of 65

Exit Quiz

Domain: Design Secure Architectures

While managing permissions for the API Gateway, what could be used to ensure that the right level of permissions is given to Developers, IT Admins, and end-users? The permissions should be easily managed.

A. Use the secure token service to manage the permissions for different users.

B. Use IAM Permissions to create different policies for different types of users.

C. Use the AWS Config tool to manage the permissions for different users.

D. Use IAM Access Keys to create sets of keys for different types of users.

Question 19 of 65

Exit Quiz

Domain: Design High-Performing Architectures

You have an Amazon Route 53 alias record that routes the traffic to an Application Load Balancer. Later on, the availability zones enabled for the load balancer are changed by a team member. When you check the load balancer using the dig command, you find that the IPs of the ELB have changed. What kind of change do you need to do for the alias record in Route 53?

- A. Change the record type from A to CNAME.
- B. Modify the destination to the DNS name of the Application Load Balancer.
- C. Add the new IP addresses in the destination of the alias record.
- D. Nothing, as Route 53 automatically recognizes changes in the resource for the alias record.

Question 20 of 65

Exit Quiz

Domain: Design High-Performing Architectures

There is an urgent requirement to monitor some database metrics for a database hosted on AWS and send notifications. Which AWS services can accomplish this? (Select TWO)

- [ ] A. Amazon Simple Email Service
- [x] B. Amazon CloudWatch
- [ ] C. Amazon Simple Queue Service
- [ ] D. Amazon Route 53
- [x] E. Amazon Simple Notification Service

Question 21 of 65

Exit Quiz

Domain: Design High-Performing Architectures

You have the following architecture deployed in AWS.

a) A set of EC2 Instances which sit behind an ELB

b) A database hosted in Amazon RDS

Of late, the performance on the database has been lacking due to a high number of read requests.

Which of the following can be added to the architecture to alleviate the given performance issue? (Select TWO)

- [x] A. Add read replica to the primary database to offload read traffic.
- [x] B. Use ElastiCache in front of the database.
- [ ] C. Use AWS CloudFront in front of the database.
- [ ] D. Use Amazon DynamoDB to offload all the reads. Populate the common read items in a separate table.

Question 22 of 65

Exit Quiz

Domain: Design Secure Architectures

You have an S3 bucket that is used to store important data for a web application. You want to receive an email notification whenever an object removal event happens in the S3 bucket. How would you configure the S3 bucket to achieve this requirement?

A. Configure the object-level logging for the S3 bucket and register an SNS topic to provide notifications.

B. Configure the server access logging for the object removal events. Add an SNS topic to notify the team via emails.

C. Set up an AWS Config rule to check the object deletion events. Register a Lambda function to send notifications.

D. Configure an S3 event notification for the object removal events. Send the events to an SNS topic.

Question 23 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

To manage a large number of AWS accounts in a better way, you create a new AWS Organization and invite multiple accounts. You only enable the "Consolidated billing" out of the two feature sets (**All features** and **Consolidated billing**) available in the AWS Organizations. Which of the following is the primary benefit of using Consolidated billing feature?

- A. Apply SCPs to restrict the services that IAM users can access.
- B. Configure tag policies to maintain consistent tags for resources in the organization's accounts.
- C. Configure a policy to prevent IAM users in the organization from disabling AWS CloudTrail.
- D. Combine the usage across all accounts to share the volume pricing discounts.

Domain: Design Secure Architectures

A Solutions Architect has been asked to design a solution that will deliver digital content to users through Amazon CloudFront. You have set up an Amazon S3 bucket as the origin and by default, CloudFront never exposes Amazon S3 URLs. The contents should only be accessed through the CloudFront distribution. How can this be achieved?

- A. Store the digital contents in the S3 bucket and create signed URLs to access S3 through CloudFront.
- B. Create OAI in CloudFront. Use the S3 bucket policy to ensure that only the OAI can access the files in the Amazon S3 bucket.
- C. Store the digital contents as private objects in the S3 buckets and use the S3 ACL to ensure that only the CloudFront distribution ARN can access the bucket.
- D. Store the digital contents in the S3 bucket and configure signed cookies for users to access contents through CloudFront.

Domain: Design Resilient Architectures

You are working as an AWS Architect for an IT Company. Your Company is using EC2 instances in multiple VPCs spanning Availability Zones in us-east-1 Region. The Development Team has deployed a new Intranet application that needs to be accessed via VPC.
You need to make sure that the connectivity to this particular application uses the internal AWS network between different VPCs, and that the solution is highly scalable and secure. Which of the following solution would you recommend?

A. Attach an Internet Gateway to all the VPCs in the us-east-1 region and allow all users to access this application over the internet.

B. Deploy Network Load Balancers along with VPC endpoint service (AWS PrivateLink) to establish connectivity between the VPCs in the us-east-1 region.

C. Use the VPC Gateway Endpoint service between all the VPCs in the us-east-1 region to provide connectivity between users & servers.

D. Create a VPN between instances at the various VPCs in the us-east-1 region to establish connectivity.

Question 26 of 65

Exit Quiz

Domain: Design Secure Architectures

You work in a large organization. Your team creates AWS resources such as Amazon EC2 dedicated hosts and reserved capacities that need to be shared by other AWS accounts. You need an AWS service to centrally manage these resources so that you can easily specify which accounts or Organizations can access the resources. Which AWS service would you choose to meet this requirement?

A. IAM

B. Resource Access Manager

C. Service Catalog

D. AWS Single Sign-On

Services

- AWS App Mesh
- Amazon Aurora
- AWS Certificate Manager Private Certificate Authority
- AWS CodeBuild
- Amazon EC2
- EC2 Image Builder
- AWS Glue
- AWS License Manager
- AWS Network Firewall
- AWS Outposts
- AWS Resource Groups
- Amazon Route 53
- Amazon VPC

Domain: Design High-Performing Architectures

Your company wants to use an S3 bucket for web hosting but has several different domains to perform operations on the S3 content. In the CORS configuration, you have added *CORSRule* AllowedOrigin for the following Domains; ***http://www.domainnamea.com***, ***https://www.secure.domainnamea.com***, and ***http://www.domainnameb.com***. Following Domains, **https://domainnameb.com** and **http://www.domainnameb.com:80**, are not allowed to access the S3 bucket.

What could be the most likely cause behind the unexpected access behaviour of the domains?

- A. Both request https://domainnameb.com and http://www.domainnameb.com:80 don't match the allowed origin in your configuration.
- B. HTTPS must contain a specific port in the request, e.g. https://domainnameb.com:443
- C. There's a limit of two origin sites per S3 bucket allowed
- D. Adding CORS automatically removes the S3 ACL and bucket policies

Question 28 of 65

Exit Quiz

Domain: Design Secure Architectures

A company has a PostgreSQL DB instance in Amazon RDS which is not encrypted. As per security policy, data in the RDS instances should be encrypted at rest with AWS KMS.

Which option is correct for RDS DB encryption?

- A. Amazon RDS for PostgreSQL DB instance can only be encrypted at creation time and not after its creation. There is no way to achieve this requirement.
- B. Take a snapshot of the unencrypted DB instance. Copy the snapshot and encrypt the new snapshot with AWS KMS. Restore the DB instance with the new encrypted snapshot.
- C. Take a snapshot of the unencrypted DB instance. Encryption can be enabled by restoring a DB instance from the unencrypted snapshot.
- D. Stop the existing RDS instance and encrypt the DB with a KMS CMK.

Domain: Design Resilient Architectures

You currently manage a set of web servers hosted on EC2 instances with public IP addresses. These IPv4 addresses are mapped to domain names. There was an urgent maintenance activity that need to be carried out on the servers. The servers had to be stopped and restarted. After the maintenance, the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this?

- A. The Route 53 hosted zone needs to be restarted.
- B. The Elastic IP address needs to be initialized again.
- C. The public IP addresses need to be associated with the ENI (Elastic network interfaces) again.
- D. The public IP addresses have changed after the instance was stopped and started again.

Question 30 of 65

Exit Quiz

Domain: Design Secure Architectures

You are responsible for deploying a critical application to AWS. It is required to monitor web application logs to identify any malicious activity. Also, there is a need to store log data in highly durable storage. Which of the following services could be used to fulfill this requirement?

- A. Amazon CloudWatch Logs
- B. AWS Personal Health Dashboard
- C. Amazon Trusted Advisor
- D. Amazon CloudTrail

Question 31 of 65

Exit Quiz

Domain: Design High-Performing Architectures

You need to deploy a high performance computing (HPC) and machine learning application in AWS Linux EC2 instances. The performance of inter-instance communication is very critical for the application. You want to attach a network device to the instance so that the computing performance can be greatly improved. Which of the following options can achieve the best performance?

- A. Enable enhanced networking feature in the EC2 instance.
- B. Configure Elastic Fabric Adapter (EFA) in the instance.
- C. Attach high speed Elastic Network Interface (ENI) in the instance.
- D. Create Elastic File System (EFS) and mount the file system in the instance.

Question 32 of 65

Exit Quiz

Domain: Design High-Performing Architectures

A company is planning on testing a large set of IoT-enabled devices. These devices will generate a large amount of data every second. You need a scalable and durable real-time data streaming service to capture the data generated from these devices. Which AWS service would be the most appropriate for this purpose?

A. AWS EMR.

B. AWS Kinesis Data Streams.

C. AWS SQS.

D. AWS SNS.

Question 33 of 65

Exit Quiz

Domain: Design Resilient Architectures

Your company currently has a set of non-production EC2 Instances hosted in AWS. To save costs, you want to stop the EC2 instance when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. Which step could be helpful to fulfill this requirement?

A. Use CloudWatch Logs to store the state change of the instances.

B. Create Amazon CloudWatch alarms that monitor the CPU utilization metric and stop the instances when the alarms are triggered.

C. Use SQS to monitor the metric and add the record to a DynamoDB table.

D. Use AWS Lambda to monitor the metric and store the state in a DynamoDB table.

Question 34 of 65

Exit Quiz

Domain: Design Secure Architectures

You have instances hosted in a private subnet in a VPC. There is a need for instances to download updates from the Internet. As an architect, what change would you suggest to the IT Operations team that would also be the most efficient and secure?

A. Create a new public subnet and move the instance to that subnet.

B. Create a new EC2 Instance to download the updates separately and then push them to the required instance.

C. Use a NAT Gateway to allow the instances in the private subnet to download the updates.

D. Create a VPC link to the Internet to allow the instances in the private subnet to download the updates.

Question 35 of 65

Exit Quiz

Domain: Design Resilient Architectures

You have an S3 bucket that receives photos uploaded by customers. When an object is uploaded, an event notification is sent to an SQS queue with the object details. You also have an ECS cluster that gets messages from the queue to do the batch processing. Each of the batch processing job takes the same amount of time to get executed. The queue size may change greatly depending on the number of incoming messages and backend processing speed. Which metric would you use to scale up/down the ECS cluster capacity?

- A. The number of messages in the SQS queue.
- B. Memory usage of the ECS cluster.
- C. Number of objects in the S3 bucket.
- D. Number of containers in the ECS cluster.

Domain: Design High-Performing Architectures

You are a solutions architect working for a regional bank that is moving its data center to the AWS cloud. You need to migrate your data center storage to a new S3 and EFS data store in AWS. Since your data includes Personally Identifiable Information (PII), you have been asked to transfer data from your data center to AWS without traveling over the public internet. Which option gives you the most efficient solution that meets your requirements?

- A. Migrate your on-prem data to AWS using the DataSync agent using NAT Gateway.
- B. Create a private VPC endpoint, and configure the DataSync agent to communicate to the private DataSync service endpoints via the VPC endpoint using Direct Connect.
- C. Migrate your on-prem data to AWS using the DataSync agent using Internet Gateway.
- D. Create a public VPC endpoint, and configure the DataSync agent to communicate to the DataSync private service endpoints via your VPC endpoint via your VPN.

Question 37 of 65

Exit Quiz

Domain: Design Secure Architectures

You have planned to host a web application on AWS. You create an EC2 Instance in a public subnet that needs to connect to an EC2 Instance that will host an Oracle database. Which steps would ensure a secure setup? (SELECT TWO)

- [ ] A. Place the EC2 Instance with the Oracle database in the same public subnet as the Webserver for faster communication.
- [x] B. Place the ec2 instance that will host the Oracle database in a private subnet.
- [x] C. Create a database Security group which allows incoming traffic only from the Web server's security group.
- [ ] D. Ensure that the database security group allows incoming traffic from 0.0.0.0/0.

Question 38 of 65

Exit Quiz

Domain: Design Secure Architectures

You are designing a website for a company that streams anime videos. You serve this content through CloudFront. The company has implemented a section for premium subscribers. This section contains more videos than the free section. You want to ensure that only premium subscribers can access this premium section. How can you achieve this easily?

- A. Using bucket policies.
- B. Requiring HTTPS for communication between users and CloudFront.
- C. Using CloudFront origin with signed URLs.
- D. Using CloudFront origin with signed cookies.

Question 39 of 65

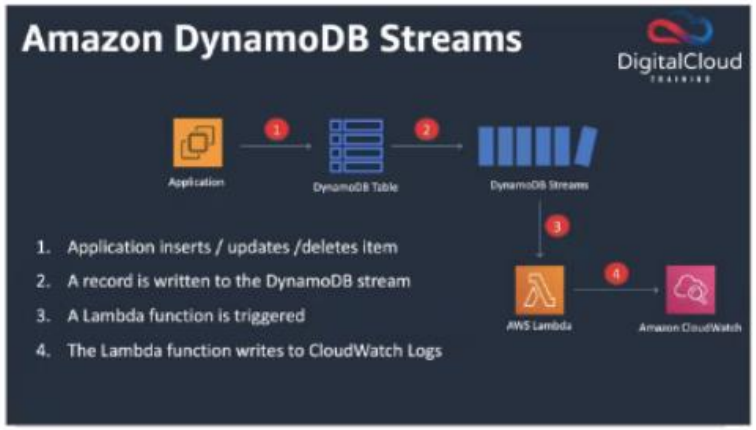
Exit Quiz

Domain: Design High-Performing Architectures

A company has set up an application in AWS that interacts with DynamoDB. It is required that when an item is modified in a DynamoDB table, an immediate entry has to be made to the associating application. How can this be accomplished? (SELECT TWO)

- [ ] A. Set up CloudWatch to monitor the DynamoDB table for changes. Then trigger a Lambda function to send the changes to the application.
- [ ] B. Set up CloudWatch logs to monitor the DynamoDB table for changes. Then trigger AWS SQS to send the changes to the application.
- [x] C. Use DynamoDB streams to monitor the changes to the DynamoDB table.
- [x] D. Trigger a lambda function to make an associated entry in the application as soon as the DynamoDB streams are modified.

show Answer



When enabled, DynamoDB Streams captures a time-ordered sequence of item-level modifications in a DynamoDB table and durably stores the information for **up to 24 hours. Applications can access a series of stream *records*, which contain an item change, from a DynamoDB stream in near real time.**

Domain: Design Resilient Architectures

You are working as an AWS consultant in an E-Commerce organization. Your organization is planning to migrate its database from on-premises data centers to Amazon RDS. The automated backup helps to restore the Database to any specific time during the backup retention period in Amazon RDS. Which of the following actions are performed as a part of the Amazon RDS automated backup process?

- A. AWS creates a storage volume snapshot of the database instance during the backup window once a day. AWS RDS also captures transactions logs and uploads them to S3 buckets every 5 minutes.
- B. AWS creates a full snapshot of the database every 12 hours during the backup window, captures transactions logs throughout the day, and stores them in S3 buckets.
- C. AWS creates a full daily snapshot during the backup window. With the snapshot, the RDS instance can be restored at any time.
- D. AWS creates a storage volume snapshot of the database instance every 12 hours during the backup window, captures transactions logs throughout the day, and stores them in S3 buckets.

Question 41 of 65

Exit Quiz

Domain: Design Secure Architectures

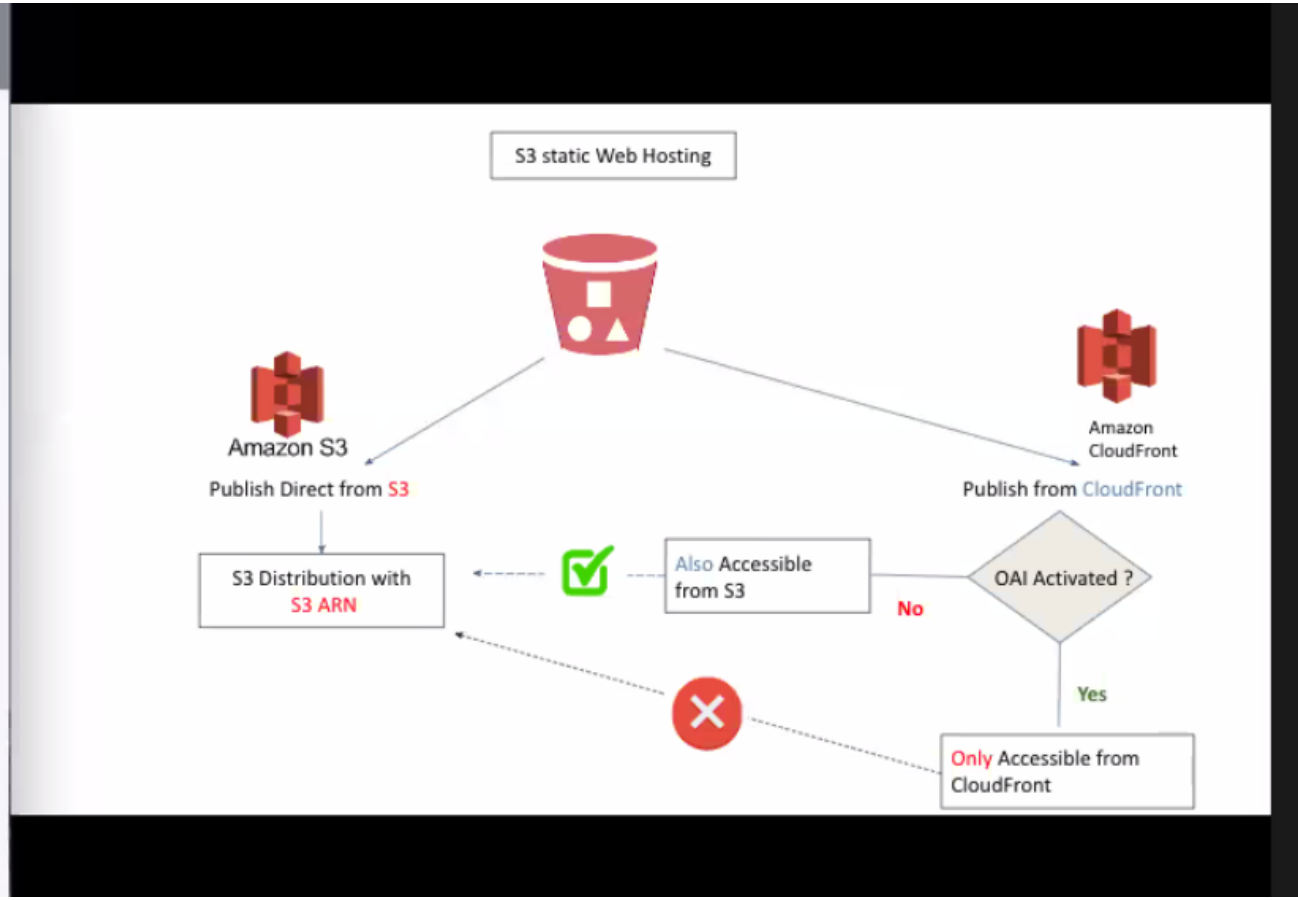
You configure an Amazon S3 bucket as the origin for a new CloudFront distribution. The traffic should not hit the S3 URLs directly instead, they should be directed to the CloudFront distribution and the files should be fetched through the CloudFront URL. Which method is the most appropriate?

A. Configure Signed URLs to serve private content by using CloudFront.

B. Configure Signed Cookies to restrict access to S3 files.

C. Create the origin access identity (OAI) and associate it with the distribution.

D. Configure the CloudFront web distribution to ask viewers to use HTTPS to request S3 objects.



As a Solutions Architect for a multinational organization with more than 150000 employees, management has decided to implement a real-time analysis for their employees' time spent in offices worldwide. You are tasked to design an architecture that will receive the inputs from 10000+ sensors with swipe machine sending in and out data across the globe, each sending 20KB data every 5 Seconds in JSON format. The application will process and analyze the data and upload the results to dashboards in real-time.

Other application requirements will include the ability to apply real-time analytics on the captured data. Processing of captured data will be parallel and durable. The application must be scalable as per the requirement as the load varies and new sensors are added or removed at various facilities. The analytic processing results are stored in a persistent data storage for data mining.

What combination of AWS services would be used for the above scenario?

A. Use EMR to copy the data coming from Swipe machines into DynamoDB and make it available for analytics.

B. Use Amazon Kinesis Data Streams to ingest the Swipe data coming from sensors, Use custom Kinesis Data Streams Applications to analyze the data and then move analytics outcomes to RedShift using AWS EMR.

C. Use SQS to receive the data coming from sensors, Kinesis Firehose to analyze the data from SQS, then save the results to a Multi-AZ RDS instance.

D. Use Amazon Kinesis Data Streams to ingest the sensors' data, Use custom Kinesis Streams applications to analyze the data, and move analytics outcomes to RDS using AWS EMR.

Domain: Design Secure Architectures

You have designed an application that uses AWS resources, such as S3, to operate and store users' documents. You currently use Cognito identity pools and user pools. To increase usage and ease of signing up, you decide that adding social identity federation is the best path forward.

How would you differentiate the Cognito identity pool and the federated identity providers (e.g., Google)?

- A. They are the same and just called different things.
- B. First, you sign-in via Cognito then through a federated site, like Google.
- C. Federated identity providers and identity pools are used to authenticate services.
- D. You can choose a federated identity provider to authenticate users and associate a Cognito identity pool to authorize the users.

Question 44 of 65

Exit Quiz

Domain: Design Resilient Architectures

You currently have your EC2 instances running in multiple availability zones in an AWS region. You need to create NAT gateways for your private instances to access internet. How would you set up the NAT gateways so that they are highly available?

- A. Create two NAT Gateways and place them behind an ELB.
- B. Create a NAT Gateway in each Availability Zone.
- C. Create a NAT Gateway in another region.
- D. Use Auto Scaling groups to scale the NAT Gateways.

Question 45 of 65

Exit Quiz

Domain: Design High-Performing Architectures

A Solutions Architect is designing an online shopping application running in a VPC on EC2 Instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The application tier must read and write data to a customer-managed database cluster. There should be no access to the database from the Internet. But the cluster must be able to obtain software patches from the Internet. Which of the following VPC design meets the requirements?

A. Create public subnets for the application tier and the database cluster.

B. Create public subnets for the application tier and private subnets for the database cluster.

C. Create public subnets with NAT Gateway for the application tier and private subnets for the database cluster.

D. Create private subnets for the application tier, and private subnets with NAT Gateway for the database cluster.

Question 46 of 65

Exit Quiz

Domain: Design High-Performing Architectures

It is expected that only certain specified customers can upload images to the S3 bucket for a certain period of time. What would you suggest as an architect to fulfill this requirement?

- A. Create a secondary S3 bucket. Then, use an AWS Lambda to sync the contents to the primary bucket.
- B. Use pre-signed URLs for uploading the images.
- C. Use ECS Containers to upload the images.
- D. Upload the images to SQS and then push them to the S3 bucket.

Question 47 of 65

Exit Quiz

Domain: Design High-Performing Architectures

You own a MySQL RDS instance in AWS Region us-east-1. The instance has a Multi-AZ instance in another availability zone for high availability. As business grows, more and more clients come from Europe (eu-west-2), and most of the database workload is read-only. What is the proper way to reduce the load on the source RDS instance?

- A. Create a snapshot of the instance and launch a new instance in eu-west-2.
- B. Promote the Multi-AZ instance to be a Read Replica and move the instance to eu-west-2 region.
- C. Configure a read-only Multi-AZ instance in eu-west-2 as Read Replicas cannot span across regions.
- D. Create a Read Replica in the AWS Region eu-west-2.

Question 48 of 65

Exit Quiz

Domain: Design Resilient Architectures

Your company manages an application that currently allows users to upload images to an S3 bucket. These images are picked up by EC2 Instances for processing and then placed in another S3 bucket. You need an area where the metadata for these images can be stored. What would be an ideal data store for this?

- A. AWS Redshift
- B. AWS Glacier
- C. AWS DynamoDB
- D. AWS SQS

Question 49 of 65

Exit Quiz

Domain: Design High-Performing Architectures

An application team needs to quickly provision a development environment consisting of a web and database layer. What would be the quickest and most ideal way to get this set up in place?

A. Create Spot Instances and install the web and database components.

B. Create Reserved Instances and install the web and database components.

C. Use AWS Lambda to create the web components and AWS RDS for the database layer.

D. Use Elastic Beanstalk to quickly provision the environment.

Question 50 of 65

Exit Quiz

Domain: Design Secure Architectures

Third-party sign-in (Federation) has been implemented in your web application to allow users who need access to AWS resources. Users have been successfully logging in using Google, Facebook, and other third-party credentials. Suddenly, their access to some AWS resources has been restricted. What is the most likely cause of the restricted use of AWS resources?

- A. IAM policies for resources were changed, thereby restricting access to AWS resources.
- B. Federation protocols are used to authorize services and need to be updated.
- C. IAM groups for accessing the AWS resources were changed, thereby restricting their access via federated login.
- D. The identity providers no longer allow access to AWS services.

Question 51 of 65

Exit Quiz

Domain: Design Secure Architectures

A security audit discovers that one of your RDS MySQL instances is not encrypted. The instance has a Read Replica in the same AWS region which is also not encrypted. You need to fix this issue as soon as possible. What is the proper way to add encryption to the instance and its replica?

- A. Create a DB snapshot from the instance. Copy the DB snapshot with encryption enabled. Restore a new DB instance from the new encrypted snapshot and configure a Read Replica in the new DB instance.
- B. Encrypt the DB instance. Launch a new Read Replica and the replica is encrypted automatically.
- C. Create a DB snapshot from the RDS instance and encrypt the newly-created snapshot. Launch a new instance and its Read Replica from the snapshot.
- D. Promote the Read Replica to be a standalone instance and encrypt it. Add a new Read Replica to the standalone instance.

A Media firm Firm_A uses AWS infrastructure and has a global presence for its sports programming & broadcasting network. It uses AWS Organization to manage multiple AWS accounts.
Recently it was acquired by Firm_B which also uses AWS Infrastructure. Firm_B also has its own sets of AWS accounts.

After the merger, AWS Accounts of both organizations need to merge to create & manage policies more effectively.

As an AWS Consultant, which of the following steps would you suggest to the client to move the management account of the Firm_A to the organization used by the merged entity? (Select THREE)

- [x] A. Remove all member accounts from the organization in Firm_A.
- [ ] B. Configure another member account as the management account in the Firm_A organization.
- [x] C. Delete the organization in Firm_A.
- [x] D. Invite the Firm_A management account to join the new organization (Firm_B) as a member account.
- [ ] E. Invite the Firm_A management account to join the new organization (Firm_B) as a management account.

Question 53 of 65

Exit Quiz

Domain: Design Secure Architectures

Your company has designed an app and requires it to store data in DynamoDB. The company has registered the app with identity providers for users to sign-in using third-parties like Google and Facebook. What must be in place such that the app can obtain temporary credentials to access DynamoDB?

- A. Multi-factor authentication must be used to access DynamoDB.
- B. AWS CloudTrail needs to be enabled to audit usage.
- C. An IAM role allowing the app to have access to DynamoDB.
- D. The user must additionally log into the AWS console to gain database access.

Question 54 of 65

Exit Quiz

Domain: Design Resilient Architectures

A company has an entire infrastructure hosted on AWS. It requires to create code templates used to provide the same set of resources in another region in case of a disaster in the primary region. Which AWS service can be helpful in this regard?

A. AWS Beanstalk

B. AWS CloudFormation

C. AWS CodeBuild

D. AWS CodeDeploy

Question 55 of 65

Exit Quiz

Domain: Design Secure Architectures

Your recent security reviews revealed a large spike in logins attempted to your AWS account. With respect to sensitive data stored in encryption enabled S3, the data has not been encrypted and is susceptible to fraud if it was to be stolen. You've recommended AWS Key Management Service as a solution. Which of the following is true regarding the operations of KMS?

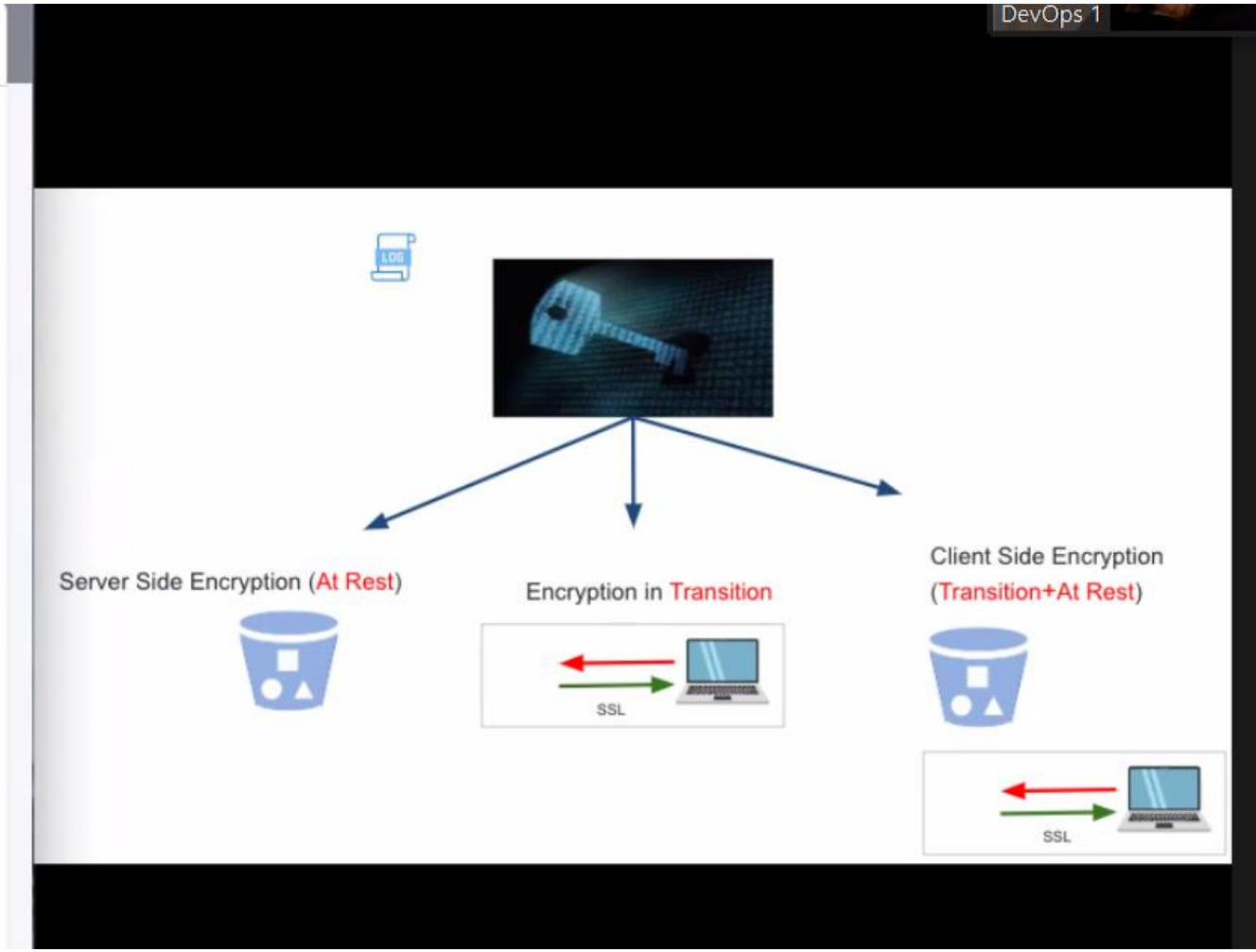
A. Only KMS generated keys can be used to encrypt or decrypt data.

B. Data is encrypted at rest with KMS.

C. KMS allows all users and roles to use the keys by default.

D. Data is encrypted in transit with the KMS key.

show Answer



Question 56 of 65

Exit Quiz

Domain: Design Resilient Architectures

Your company has a set of EC2 Instances hosted in AWS. It is required to prepare for regional disasters and come up with the necessary disaster recovery procedures. Which of the following steps would help to mitigate the effects of disaster in the future on EC2 Instances?

- A. Place an ELB in front of the EC2 Instances.
- B. Use Auto Scaling to ensure that the minimum number of instances are always running.
- C. Use CloudFront in front of the EC2 Instances.
- D. Create AMIs from the EC2 Instances. Use them to recreate the EC2 Instances in another region.

Your company currently has setup their data store on AWS DynamoDB. One of your main revenue generating applications uses the tables in this service. Your application is now expanding to 2 different other locations and you want to ensure that the latency for data retrieval is the least from the new regions. Which of the following can help accomplish this?

- A. Place a cloudfront distribution in front of the database
- B. Enable Multi-AZ for DynamoDB
- C. Place an ElastiCache in front of DynamoDB
- D. Enable global tables for DynamoDB

A start-up firm is using an AWS Organization for managing policies across its Development and Production accounts. The development account needs an EC2 dedicated host. The Production account has subscribed to an EC2 dedicated host for its application but is not currently using it. Sharing has NOT been enabled with the AWS Organization in AWS RAM.

Which of the following can be done to share the Amazon EC2 dedicated host from the Production account to the Development account?

- A. Remove both Development & Production Accounts from Organization & then share resources between them.
- B. Resources in the same organization are automatically shared without the need to accept the invitation of sharing resources.
- C. Create a resource share in the production account and accept the invitation in the development account.
- D. Remove the destination Development account from an Organization & then share resources with it.

Question 59 of 65

Exit Quiz

Domain: Design High-Performing Architectures

A company has a lot of data hosted on their On-premises infrastructure. Running out of storage space, the company wants a quick win solution using AWS. There should be low latency for the frequently accessed data. Which of the following would allow the easy extension of their data infrastructure to AWS?

- A. The company could start using Gateway Cached Volumes.
- B. The company could start using Gateway Stored Volumes.
- C. The company could start using the Amazon S3 Glacier Deep Archive storage class.
- D. The company could start using Amazon S3 Glacier.

Exit Quiz

Domain: Design Resilient Architectures

A Large Medical Institute is using a legacy database for saving all its patient details. Due to compatibility issues with the latest software, they plan to migrate this database to AWS cloud infrastructure. This large size database will be using a NoSQL database Amazon DynamoDB in AWS. As an AWS consultant, you need to ensure that all the current legacy database tables are migrated without a glitch to Amazon DynamoDB. Which of the following is the most cost-effective way of transferring legacy databases to Amazon DynamoDB?

- A. Use AWS DMS with AWS Schema Conversion Tool to save data to Amazon S3 bucket & then upload all data to Amazon DynamoDB.
- B. Use AWS DMS with engine conversion tool to save data to Amazon S3 bucket & then upload all data to Amazon DynamoDB.
- C. Use AWS DMS with engine conversion tool to save data to Amazon EC2 & then upload all data to Amazon DynamoDB.
- D. Use AWS DMS with AWS Schema Conversion Tool to save data to Amazon EC2 instance & then upload all data to Amazon DynamoDB.

A Financial firm is planning to build a highly resilient application with primary database servers located at on-premises data centers while maintaining its DB snapshots in an S3 bucket. The IT Team is looking for a cost-effective and secure way of transferring the large customer financial databases from on-premises servers to the Amazon S3 bucket with no impact on the client usage of these applications. Also, post this data transfer, the on-premises application will be fetching data from the Amazon S3 bucket in case of a primary database failure.

So, your solution should ensure that the Amazon S3 data is fully synced with the on-premises database. Which of the following can be used to meet this requirement?

- A. Use Amazon S3 Transfer Acceleration for transferring data between the on-premises & Amazon S3 bucket while using AWS Data Sync for accessing these S3 bucket data from the on-premises application.
- B. Use AWS Data Sync for transferring data between the on-premises & Amazon S3 bucket while using AWS Storage Gateway for accessing these S3 bucket data from the on-premises application.
- C. Use AWS Snowball Edge for transferring data between the on-premises & Amazon S3 bucket while using AWS Storage Gateway for accessing these S3 bucket data from the on-premises application.
- D. Use AWS Transfer for transferring data between the on-premises & Amazon S3 bucket while using AWS Data Sync for accessing these S3 bucket data from the on-premises application.

Question 62 of 65

Exit Quiz

Domain: Design Cost-Optimized Architectures

A company has an application that delivers objects from S3 to global users. Of late, some users have been complaining of slow response times. Which additional step would help to build a cost-effective solution and ensure that the users get an optimal response to objects from S3?

- A. Use S3 Replication to replicate the objects to regions closest to the users.
- B. Ensure S3 Transfer Acceleration is enabled to ensure that all users get the desired response times.
- C. Place an ELB in front of S3 to distribute the load across S3.
- D. Place the S3 bucket behind a CloudFront distribution.

A large IT company is using Amazon CloudFront for its web application. Static Content for this application is saved in the Amazon S3 bucket. Amazon CloudFront is configured for this application to provide faster access to these files for global users.

IT Team is concerned about some critical files that need to be accessed only by users from certain white-list countries that you have defined in Amazon CloudFront geo-restriction. There is a requirement that no users should access these files directly using the Amazon S3 URL. Which of the following is the best way to achieve the given requirement?

- (●) **A.** Create an OAI user to associate with distribution & modify permission on Amazon S3 bucket using bucket policy.
- ( ) **B.** Create Amazon CloudFront Signed URLs to limit access to these files & modify permission on Amazon S3 bucket using bucket policy.
- ( ) **C.** Create an OAI user to associate with distribution & modify permission on Amazon S3 bucket using object ACL's.
- ( ) **D.** Create Amazon CloudFront Signed URLs to limit access to these files & modify permission on Amazon S3 bucket using object ACL's.

Domain: Design Secure Architectures

A start-up firm has a corporate office in New York & a regional office in Washington & Chicago. These offices are interconnected over Internet links. Recently they have migrated a few application servers to EC2 instance launched in the AWS US-east-1 region. The Developer Team located at the corporate office requires secure access to these servers for initial testing & performance checks before go-live of the new application. Since the go-live date is approaching soon, the IT team is looking for quick connectivity to be established. As an AWS consultant, which link option will you suggest as a cost-effective & quick way to establish secure connectivity from on-premise to servers launched in AWS?

- A. Use AWS Direct Connect to establish IPSEC connectivity from On-premise to VGW.
- B. Install a third party software VPN appliance from AWS Marketplace in the EC2 instance to create a VPN connection to the on-premises network.
- C. Use Hardware VPN over AWS Direct Connect to establish IPSEC connectivity from On-premise to VGW.
- D. Use AWS Site-to-Site VPN to establish IPSEC VPN connectivity between VPC and the on-premises network.

Question 65 of 65

Exit Quiz

Domain: Design Secure Architectures

You are a Solutions Architect in a startup company that is releasing the first iteration of its app. Your company doesn't have a directory service for its intended users but wants the users to sign in and use the app. Which of the following solutions is the most cost-efficient?

- A. Create an IAM role for each end user and the user will assume the IAM role when he signs in the APP.
- B. Create an AWS user account for each customer.
- C. Invest heavily in Microsoft Active Directory as it's the industry standard.
- D. Use Cognito Identity along with a User Pool to securely save users' profile attributes.