

### Question #341

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
- B.** Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
- C.** Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.
- D.** Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

## Question #342

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run. Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.
- B.** Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.
- C.** Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.
- D.** Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

### Question #343

A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
- B.** Migrate the MySQL database to Amazon RD
- S.** Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
- C.** Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
- D.** Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

### Question #344

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB. Which solution will meet these requirements with the FEWEST changes to the code?

- A.** Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- B.** Use Amazon EventBridge to post large messages from the application instead of Amazon SQ
- S.**
- C.** Change the limit in Amazon SQS to handle messages that are larger than 256 K
- B.**
- D.** Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

### Question #345

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible. Which solution will meet these requirements MOST cost-effectively?

- A.** Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B.** Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C.** Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
- D.** Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

### **Question #346**

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive. A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution. Which type of storage gateway should the solutions architect provision to meet these requirements?

- A.** Volume Gateway
- B.** Tape Gateway
- C.** Amazon FSx File Gateway
- D.** Amazon S3 File Gateway

### **Question #347**

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company. The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage. Which solution will meet these requirements MOST cost-effectively?

- A.** Compute Savings Plan
- B.** EC2 Instance Savings Plan
- C.** Zonal Reserved Instances
- D.** Standard Reserved Instances

### Question #348

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB. Which solution will meet these requirements MOST cost-effectively?

- A.** Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
- B.** Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
- C.** Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
- D.** Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.



### Question #349

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3. What should a solutions architect do to meet these requirements?

- A.** Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.
- B.** Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.
- C.** Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.
- D.** Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

### Question #350

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance. The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process. Which combination of steps will meet these requirements? (Choose two.)

- A.** Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
- B.** Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
- C.** Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.
- D.** Migrate the database to RDS Custom.
- E.** Use RDS Proxy to limit reporting requests to the maintenance window.

### Question #351

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead. Which solution will meet these requirements?

- A.** Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.
- B.** Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.
- C.** Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
- D.** Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

### Question #352

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.** Setup 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.

### Question #353

A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic. The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant. Which solution will meet these requirements MOST cost-effectively?

- A.** Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
- B.** Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
- C.** Use Amazon S3 Intelligent-Tiering access tiers.
- D.** Use two large EC2 instances to host the database in active-passive mode.

### Question #354

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code. What should a solutions architect do to meet these requirements?

- A.** Reduce the Lambda concurrency rate.
- B.** Enable RDS Proxy on the RDS DB instance.
- C.** Resize the RDS DB instance class to accept more connections.
- D.** Migrate the database to Amazon DynamoDB with on-demand scaling.

### Question #355

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory. Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

- A. Use AWS Lambda with functional scaling.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- C. Use Amazon Lightsail with AWS Auto Scaling.
- D. Use AWS Batch on Amazon EC2.

### Question #356

A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs. Which storage solution will meet these requirements?

- A.** Move the data objects to S3 Glacier Deep Archive after 30 days.
- B.** Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C.** Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D.** Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.



### Question #357

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code. Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A.** Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
- B.** Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
- C.** Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
- D.** Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
- E.** Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

### Question #358

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Install an external image management library on an EC2 instance. Use the image management library to process the images.
- B.** Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
- C.** Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
- D.** Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

### Question #359

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest. Which solution will meet these requirements?

- A.** Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- B.** Use the `aws:SecureTransport` condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
- C.** Use the `aws:SecureTransport` condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- D.** Use the `aws:SecureTransport` condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

### Question #360

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC. Which solution will meet these requirements with the FEWEST changes to the code?

- A. Add an X-API-Key header in the HTTP header for authorization.
- B. Use an interface endpoint.
- C. Use a gateway endpoint.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

### Question #361

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
- B.** Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- C.** Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- D.** Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

### Question #362

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly. Which actions should a solutions architect take to meet this requirement? (Choose two.)

- A.** Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
- B.** Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C.** Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
- D.** Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
- E.** Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

### **Question #363**

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events. Which solution will meet these requirements?

- A.** Amazon EventBridge event bus
- B.** Amazon Simple Notification Service (Amazon SNS) FIFO topics
- C.** Amazon Simple Notification Service (Amazon SNS) standard topics
- D.** Amazon Simple Queue Service (Amazon SQS) FIFO queues

### Question #364

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture. A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A.** Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.
- B.** Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.
- C.** Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.
- D.** Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.
- E.** Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.



### **Question #365**

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days. Which feature should the solutions architect include in the design to meet this requirement?

- A.** Read replicas
- B.** Manual snapshots
- C.** Automated backups
- D.** Multi-AZ deployments

### Question #366

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content. Which solution will meet this requirement with the LEAST operational overhead?

- A.** Enable API caching and throttling on the API Gateway AP  
I.
- B.** Set up AWS WAF on the API Gateway AP  
I. Create a rule to filter users who have a subscription.
- C.** Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
- D.** Implement API usage plans and API keys to limit the access of users who do not have a subscription.

### Question #367

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application. What should a solutions architect do to meet these requirements?

**A.** Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DN

S.

**B.** Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DN

S.

**C.** Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DN

S.

**D.** Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

### **Question #368**

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A.** Set an overall password policy for the entire AWS account.
- B.** Set a password policy for each IAM user in the AWS account.
- C.** Use third-party vendor software to set password requirements.
- D.** Attach an Amazon CloudWatch rule to the Create\_newuser event to set the password with the appropriate requirements.

### Question #369

A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
- B.** Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
- C.** Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
- D.** Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

### Question #370

A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance. Which solution meets these requirements?

- A.** Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- B.** Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- C.** Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
- D.** Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

### Question #371

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS). Which combination of actions will meet this requirement with the LEAST operational overhead? (Choose two.)

- A.** Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
- B.** After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
- C.** Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
- D.** Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
- E.** Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

### Question #372

A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code. When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events. Which solution meets these requirements MOST cost-effectively?

- A.** Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
- B.** Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
- C.** Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
- D.** Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.



### Question #373

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models. Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes. Which storage solution meets these requirements MOST cost-effectively?

- A.** Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B.** Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C.** Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D.** Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

### Question #374

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center. A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness. Which solution meets these requirements?

- A.** Configure three AWS Site-to-Site VPN connections from the data center to AWS
- S.** Establish connectivity by configuring one VPN connection for each VPC
- C.**
- B.** Launch a third-party virtual network appliance in each VPC
- C.** Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C.** Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
- D.** Set up one AWS Direct Connect connection from the data center to AWS
- S.** Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

### Question #375

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Which solution will meet these requirements with the LEAST operational overhead?

- A.** Use AWS Step Functions to build the application.
- B.** Integrate all the application components in an AWS Glue job.
- C.** Use Amazon Simple Queue Service (Amazon SQS) to build the application.
- D.** Use AWS Lambda functions and Amazon EventBridge events to build the application.

### Question #376

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors. Which solution will resolve this issue with the LEAST operational overhead?

- A.** Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
- B.** Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.
- C.** Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
- D.** Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

### Question #377

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated. Which solution achieves these goals MOST efficiently?

- A.** Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B.** Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C.** Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D.** Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

### Question #378

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention. Which solution should a solutions architect recommend?

- A.** Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B.** Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C.** Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D.** Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

### Question #379

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations. Which solution will meet these requirements?

- A.** Establish a connection between the frontend application and the database to make queries faster by bypassing the AP  
I.
- B.** Configure provisioned concurrency for the Lambda function that handles the requests.
- C.** Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
- D.** Increase the size of the database to increase the number of connections Lambda can establish at one time.

### Question #380

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance. Which solution will meet these requirements?

- A.** Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.
- B.** Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.
- C.** Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
- D.** Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.



### Question #381

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently. The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process. Which solution will meet these requirements with the LEAST amount of change to the application code?

- A.** Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
- B.** Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- C.** Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- D.** Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

### Question #382

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database. What should a solutions architect do to improve the security of the data in transit?

- A.** Configure a TLS listener. Deploy the server certificate on the NLB.
- B.** Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
- C.** Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
- D.** Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

### **Question #383**

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year. Which Amazon EC2 pricing option is the MOST cost-effective?

- A. Dedicated Reserved Hosts**
- B. Dedicated On-Demand Hosts**
- C. Dedicated Reserved Instances**
- D. Dedicated On-Demand Instances**

### Question #384

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time. Which solution will meet these requirements MOST cost-effectively?

- A.** Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
- B.** Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
- C.** Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
- D.** Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

### Question #385

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks. Which additional configuration strategy should the solutions architect use to meet these requirements?

- A.** Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B.** Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C.** Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D.** Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

### **Question #386**

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns. Which action should be taken to improve the performance of the backend?

- A.** Implement Amazon SNS to store the database calls.
- B.** Implement Amazon ElastiCache to cache the large datasets.
- C.** Implement an RDS for MySQL read replica to cache database calls.
- D.** Implement Amazon Kinesis Data Firehose to stream the calls to the database.

### Question #387

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege. Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A.** Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B.** Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C.** Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.
- D.** Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E.** Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

### Question #388

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information. The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states. What should a solutions architect recommend to fix the application?

- A.** Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B.** Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C.** Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D.** Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tiers security group.



### Question #389

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance. Which solution meets these requirements?

- A.** Deploy RDS read replicas to process the business reporting queries.
- B.** Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.
- C.** Scale up the DB instance to a larger instance type to handle write operations and queries.
- D.** Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

### Question #390

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance. The company wants to optimize customer session management during transactions. The application must store session data durably. Which solutions will meet these requirements? (Choose two.)

- A.** Turn on the sticky sessions feature (session affinity) on the ALB.
- B.** Use an Amazon DynamoDB table to store customer session information.
- C.** Deploy an Amazon Cognito user pool to manage user session information.
- D.** Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E.** Use AWS Systems Manager Application Manager in the application to manage user session information.

### Question #391

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours. The backup strategy must maximize scalability and optimize resource utilization for this environment. Which solution will meet these requirements?

- A.** Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
- B.** Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
- C.** Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
- D.** Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

## Question #392

A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance. The application must be secure and accessible for global customers that have dynamic IP addresses. How should a solutions architect configure the security groups to meet these requirements?

- A.** Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- B.** Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- C.** Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
- D.** Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

### Question #393

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers. What should a solutions architect do to meet these requirements?

- A.** Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.
- B.** When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
- C.** Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
- D.** Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.

### Question #394

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand. A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000. What should a solutions architect do to improve the application performance?

- A.** Replace the volume with a magnetic volume.
- B.** Increase the number of IOPS on the gp3 volume.
- C.** Replace the volume with a Provisioned IOPS SSD (io2) volume.
- D.** Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

### **Question #395**

An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes. Which service should the solutions architect use to find the desired information?

- A.** Amazon GuardDuty
- B.** Amazon Inspector
- C.** AWS CloudTrail
- D.** AWS Config

### Question #396

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in 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.



### Question #397

An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance. A solutions architect needs to minimize the amount of operational effort that is needed for the job to run. Which solution meets these requirements?

- A.** Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
- B.** Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
- C.** Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
- D.** Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

### Question #398

A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps. Which solution meets these requirements MOST cost-effectively?

- A.** Use Amazon S3 multi-part upload functionality to transfer the files over HTTP S.
- B.** Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
- C.** Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
- D.** Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

### Question #399

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline. A solutions architect must design a solution to protect the application from this type of attack. Which solution meets these requirements with the LEAST operational overhead?

- A.** Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B.** Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C.** Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D.** Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

### Question #400

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application. What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A.** Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B.** Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C.** Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D.** Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

## Question #401

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage. The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand. Which solution will meet these requirements?

- A.** Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.
- B.** Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database on an EC2 instance. Enable EC2 Auto Recovery.
- C.** Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.
- D.** Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones. Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

### Question #402

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams. What should a solutions architect do to resolve this issue?

- A.** Update the Kinesis Data Streams default settings by modifying the data retention period.
- B.** Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C.** Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D.** Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

### Question #403

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3. What should a solutions architect do to grant the permissions?

- A.** Add required IAM permissions in the resource policy of the Lambda function.
- B.** Create a signed request using the existing IAM credentials in the Lambda function.
- C.** Create a new IAM user and use the existing IAM credentials in the Lambda function.
- D.** Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

### Question #404

A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents. What should a solutions architect do to improve the architecture of this application?

- A.** Set the Lambda function's runtime timeout value to 15 minutes.
- B.** Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing.
- C.** Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.
- D.** Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.



### Question #405

A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends. Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two.)

- A.** Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
- B.** Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
- C.** Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
- D.** Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
- E.** Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

### Question #406

A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A.** Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.
- B.** Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.
- C.** Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
- D.** Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.
- E.** Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.

### Question #407

A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution must be fully managed. Which solution meets these requirements?

- A.** Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B.** Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- C.** Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D.** Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

## Question #408

A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored. The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region. Which solution will meet these requirements?

**A.** Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.

**B.** Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB to process the data in Amazon EC2.

S.

**C.** Use AWS Global Accelerator. Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB.

**B.** Process the data in Amazon EC2.

S.

**D.** Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB.

**B.** Process the data in Amazon ECS.

### Question #409

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances. Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file share to Amazon RD S.
- B. Migrate the file share to AWS Storage Gateway.
- C. Migrate the file share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS).

## Question #410

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest. Which solution will meet this requirement?

- A.** Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.
- B.** Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
- C.** Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.
- D.** Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.

### **Question #411**

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications. Which solution will meet these requirements?

- A.** Amazon DynamoDB
- B.** Amazon RDS for MySQL
- C.** MySQL-compatible Amazon Aurora Serverless
- D.** MySQL deployed on Amazon EC2 in an Auto Scaling group

## Question #412

An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private. Which solution will meet these requirements?

- A.** Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
- B.** Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.
- C.** Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
- D.** Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.



### Question #413

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead. What should a solutions architect do to meet these requirements?

- A.** Create a separate application tier using EC2 instances dedicated to email processing.
- B.** Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C.** Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D.** Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

### Question #414

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis. Which solution will meet these requirements with the LEAST administrative overhead?

- A.** Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
- B.** Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
- C.** Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
- D.** Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

### Question #415

A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage. Which solution will meet these requirements with the MOST operational efficiency?

- A.** Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
- B.** Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
- C.** Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
- D.** Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

### Question #416

A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads. Which combination of actions should a solutions architect take to resolve this issue? (Choose two.)

- A. Configure an Amazon Redshift cluster.
- B. Set up an Amazon CloudFront distribution.
- C. Host the dynamic web content in Amazon S3.
- D. Create a read replica for the RDS DB instance.
- E. Configure a Multi-AZ deployment for the RDS DB instance.

## Question #417

A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work. The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low. Which solution will meet these requirements?

- A.** Purchase an EC2 Instance Savings Plan. Optimize the Lambda functions' duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- B.** Purchase an EC2 Instance Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
- C.** Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- D.** Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.

### Question #418

A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account. The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account. Which solution will meet these requirements while complying with the principle of least privilege?

- A.** Attach the Administrator Access policy to the development account users.
- B.** Add the development account as a principal in the trust policy of the role in the production account.
- C.** Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
- D.** Create a user in the production account with unique credentials for each team member.

## Question #419

A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest. An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any IAM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes. Which combination of steps will meet these requirements? (Choose two.)

- A.** In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.
- B.** Create an IAM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the `ec2:CreateVolume` action when the `ec2:Encrypted` condition equals false.
- C.** Create an SC
- P.** Attach the SCP to the root organizational unit (OU). Define the SCP to deny the `ec2:CreateVolume` action when the `ec2:Encrypted` condition equals false.
- D.** Update the IAM policies for each account to deny the `ec2:CreateVolume` action when the `ec2:Encrypted` condition equals false.
- E.** In the Organizations management account, specify the Default EBS volume encryption setting.

## Question #420

A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible. Which solution will meet these requirements?

- A.** Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.
- B.** Use an Amazon RDS Multi-AZ DB cluster deployment. Create two read replicas and point the read workload to the read replicas.
- C.** Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.
- D.** Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.



## Question #421

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers. The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions. Which solution will meet these requirements?

- A.** Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- B.** Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- C.** Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.
- D.** Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

## Question #422

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent. The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time. Which design should a solutions architect recommend to meet these requirements?

- A.** Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NL
- B.**
- B.** Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.
- C.** Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.
- D.** Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.

### Question #423

A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions: Which IAM principals can the solutions architect attach this policy to? (Choose two.)

- A. Role
- B. Group
- C. Organization
- D. Amazon Elastic Container Service (Amazon ECS) resource
- E. Amazon EC2 resource

### Question #424

A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day. The company needs to scale out and scale in more instances based on workload. Which solution will meet these requirements MOST cost-effectively?

- A.** Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
- B.** Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.
- C.** Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
- D.** Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

### **Question #425**

A company uses high block storage capacity to runs its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity. Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?

- A.** GP2 volume type
- B.** io2 volume type
- C.** GP3 volume type
- D.** io1 volume type