COHORT 3

AWS SOLUTIONS ARCHITECT ASSOCIATE PRACTICE QUESTIONS 1

105 QUESTIONS

Question 1
A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received. Which solution will meet these requirements?

A. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing. **Correct answer**

C. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.

D. Use an API Gateway authorizer to block any requests while the application processes an order.

Overall explanation
Amazon SQS FIFO Queue: Using an Amazon SQS FIFO queue ensures that messages are processed in the order they are received. "FIFO" stands for First-In-First-Out, and it guarantees the order of processing for messages.

API Gateway Integration: Option B utilizes API Gateway for integration, which means you can seamlessly send order information to the SQS FIFO queue as soon as the application receives an order.

AWS Lambda for Processing: AWS Lambda is well-suited for processing messages from SQS queues. By configuring the SQS FIFO queue to invoke an AWS Lambda function, you can efficiently process orders as they arrive.

Question 2
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 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.

B. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.

C. 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.

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.
Correct answer

Overall explanation
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.

Explanation:

Scalability with SQS: Using SQS as a message queue allows for decoupling between components, providing scalability and asynchronous processing.

ECS for Microservices: Deploying the models as ECS services enables efficient containerized execution of microservices, ensuring resource isolation and flexibility.

Auto Scaling Based on Queue Size: Enabling AWS Auto Scaling on ECS allows for dynamic scaling of both the ECS cluster and service instances based on the size of the SQS queue.

Efficient Resource Utilization: Auto Scaling ensures that resources are scaled up or down based on demand, optimizing resource utilization.

Irregular Usage Patterns: This solution accommodates irregular usage patterns and efficiently handles varying workloads without continuous running of backend nodes.

Question 3
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. MySQL deployed on Amazon EC2 in an Auto Scaling group

B. Amazon RDS for MySQL

C. Amazon DynamoDB

D. MySQL-compatible Amazon Aurora Serverless **Correct answer**

Overall explanation
MySQL-compatible Amazon Aurora Serverless

Explanation:

Sporadic Usage Patterns: Aurora Serverless automatically adjusts capacity based on actual usage, making it suitable for applications with unpredictable usage patterns.

Cost-Effective: Aurora Serverless offers automatic scaling, and you pay for the database capacity (measured in Aurora Capacity Units, ACUs) only when the capacity is in use.

No Database Modifications: Aurora is MySQL-compatible, allowing for a seamless migration without the need for database modifications.

High Availability: Aurora Serverless provides high availability with automatic failover, ensuring that the database remains available even in the event of a failure.

Serverless Model: With Aurora Serverless, there is no need to provision or manage database instances continuously, reducing operational overhead.

Question 4

A company has a data ingestion workflow that consists of the following:
• An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
• An AWS Lambda function to process the data and record metadata
The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

A. Increase provisioned throughput for the Lambda function.

B. Increase the CPU and memory that are allocated to the Lambda function.

C. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic. **Correct answer**

D. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue. **Correct answer**

E. Deploy the Lambda function in multiple Availability Zones.

Overall explanation

Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic:

By creating an SQS queue and subscribing it to the SNS topic, you decouple the processing of messages from the publisher (SNS). This means that even if network connectivity issues or temporary failures occur, messages published to the SNS topic are stored in the SQS queue, and the Lambda function can retrieve and process them when it's able to do so. This ensures that no data is lost.

Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue:

By having the Lambda function read from an SQS queue, you can ensure that the Lambda function processes all messages, even if there are network issues or occasional failures. The SQS queue acts as a buffer, allowing the Lambda function to process messages at its own pace without data loss.

Question 5

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

A. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket. run an AWS Lambda function to process the data for analysis.

B. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.

C. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.

D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.**Correct answer**

Overall explanation

Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Explanation:

Amazon Kinesis is designed for real-time data streaming and is suitable for collecting, processing, and analyzing large volumes of streaming data such as clickstream data. Amazon Kinesis Data Firehose can be used to easily capture and load data into an Amazon S3 data lake.

In this scenario, you can collect the clickstream data from Amazon Kinesis Data Streams, use Amazon Kinesis Data Firehose to efficiently transmit and load the data into an Amazon S3 data lake. This data can then be processed and analyzed using Amazon Redshift for your analytics needs.

This architecture is well-suited for processing large volumes of streaming data efficiently and allows you to perform analytics on the stored data.

Question 6

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

A. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.

C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream. **Correct answer**

D. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.

Overall explanation

This solution leverages the real-time capabilities of Amazon Kinesis Data Streams and AWS Lambda to process and store the transactions data while ensuring that sensitive information is removed.

Kinesis Data Streams allows you to ingest and process high volumes of streaming data, and you can use AWS Lambda to perform data transformation and cleaning operations as data flows through the stream.

After removing sensitive data, the cleaned transactions can be stored in Amazon DynamoDB for low-latency retrieval, and other applications can consume the processed data from the Kinesis data stream.

This architecture is scalable, near-real-time, and well-suited for high-throughput and sensitive data processing.

Question 7
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. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.

B. 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.

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. **Correct answer**

D. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.

Overall explanation
AWS Snowball Edge is a physical data transfer appliance that can be used to transfer large amounts of data from on-premises to AWS. It is suitable for situations where the data transfer over the network is not feasible.

The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly.

Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

Question 8
Skipped
A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

B. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.Correct answer

C. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.Correct answer

D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.

E. Configure the application to send the data to Amazon Kinesis Data Firehose.

Overall explanation
So, the combination of steps you should take to meet these requirements is:

Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.

Use Amazon Simple Email Service (Amazon SES) to format the data and send the report by email.

Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event:

Use Amazon EventBridge to schedule an event to trigger a specific action at the desired time each morning. For this use case, create a scheduled event to trigger the data extraction process.

Use an AWS Lambda function to query the application's API for the data:

Configure the Amazon EventBridge event to trigger an AWS Lambda function at the scheduled time. The Lambda function can make API calls to the application to extract the shipping statistics.

Organize the data into an HTML report:

Inside the Lambda function, you can process and format the extracted data into an HTML report. You can use various Node.js libraries like Mustache, Handlebars, or other HTML templating tools for this purpose.

Send the report by email using Amazon Simple Email Service (Amazon SES):

After generating the HTML report, you can use Amazon SES to send the HTML-formatted report to the multiple email addresses. Configure your Lambda function to use Amazon SES to send the email to the specified recipients.

Question 9

A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.
What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

A. Deploy a gateway VPC endpoint for Amazon S3. **Correct answer**

B. Replace the NAT gateway with a NAT instance.

C. Provision an EC2 Dedicated Host to run the EC2 instances.

D. Launch the NAT gateway in each Availability Zone.

Overall explanation
A VPC endpoint for Amazon S3 allows the EC2 instances to access Amazon S3 within the same region without incurring data transfer charges. It routes traffic to Amazon S3 directly from the VPC, avoiding the need to go through the NAT gateway.

Launching a NAT gateway in each Availability Zone (option A) or replacing the NAT gateway with a NAT instance (option B) would not eliminate data transfer charges, as the data would still have to pass through the NAT device to reach Amazon S3.

Provisioning an EC2 Dedicated Host (option D) does not address the data transfer charges and is not related to reducing data transfer costs between the EC2 instances and Amazon S3.

Question 10

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. 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. **Correct answer**

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. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.

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.

Overall explanation

Enabling DynamoDB Streams allows you to capture changes to the DynamoDB table, and you can use triggers to write to an Amazon SNS topic. This allows teams to subscribe to a single topic for notifications with minimal operational overhead.

The best solution to meet these requirements with the least amount of operational overhead is to enable Amazon DynamoDB Streams on the table and use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.

This solution requires minimal configuration and infrastructure setup, and Amazon DynamoDB Streams provide a low-latency way to capture changes to the DynamoDB table. The triggers automatically capture the changes and publish them to the SNS topic, which notifies the internal teams.

Question 11

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.**Correct answer**

B. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.

C. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.

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

Overall explanation
AWS Shield Advanced provides advanced DDoS protection. Adding the accelerator as a resource allows it to be protected against DDoS attacks.

Question 12

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 Config

D. AWS CloudTrail **Correct answer**

Overall explanation
AWS CloudTrail is the service used to monitor and log AWS API call activity. It records API actions taken on AWS resources, including who performed the actions.

Question 13

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.

B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.

C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server. **Correct answer**

D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Overall explanation

Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.

Here's why this option is the most suitable:

Amazon FSx for Windows File Server: FSx for Windows File Server is a managed file storage service that is fully compatible with Windows file shares. It's designed to work with Windows-based applications and environments.

Multi-AZ Configuration: Amazon FSx supports Multi-AZ configurations, which means that it replicates your data across multiple Availability Zones for high availability and durability.

Data Migration: You can migrate the existing data from your EC2 instances to FSx for Windows File Server.

This solution provides a highly available and durable storage environment while preserving the way users currently access the files using Windows file shares. It's a good fit for Windows workloads and offers native Windows compatibility.

Question 14

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

A. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months. **Correct answer**

B. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

C. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.

D. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.

Overall explanation
AWS Billing and Cost Management dashboard provides a built-in interface for generating cost and usage reports without the need to create custom reports or set up additional tools.

You can easily create graphs and visualize cost data, including EC2 costs based on instance types, directly from the AWS Management Console.

This approach is user-friendly and does not require setting up additional services or performing complex configurations.

Question 15

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency.

Which solution will meet these requirements?

A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.

B. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years. **Correct answer**

C. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.

D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Overall explanation
Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

Here's why this option is the most appropriate:

S3 Object Lock: S3 Object Lock ensures that objects remain unaltered for the duration you specify. In this case, you want to retain the records without deletion for 10 years, which is precisely what S3 Object Lock in compliance mode is designed for.

S3 Lifecycle Policy: Using an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year helps to reduce storage costs. It's a cost-effective way to manage data retention while keeping the records accessible for the required period.

S3 Glacier Deep Archive: S3 Glacier Deep Archive provides durable, secure, and cost-effective archival storage for long-term data retention.

This solution ensures that the records are immediately accessible for 1 year in S3 Standard, followed by secure and durable archival storage in S3 Glacier Deep Archive for the additional 9 years. Additionally, it enforces the restriction on deletion, making it suitable for the company's needs.

Question 16

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. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

B. Update the Kinesis Data Streams default settings by modifying the data retention period.

C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.**Correct answer**

D. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.

Overall explanation

Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.

Explanation:

Kinesis Data Streams use shards to scale throughput. If data is not reaching Amazon S3, it may be because the number of shards is insufficient.

Increasing the number of Kinesis shards allows for greater parallel processing and can handle higher data throughput.

Updating the Kinesis Data Streams configuration to match the required throughput is essential to ensure that all data is ingested.

Question 17

A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.

What should a solutions architect do to meet this requirement?

A. Update the ALB's network ACL to accept only HTTPS traffic.

B. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS. **Correct answer**

D. Create a rule that replaces the HTTP in the URL with HTTPS.

Overall explanation
Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

Explanation:

To ensure that all HTTP requests are redirected to HTTPS, you should create a listener rule on the Application Load Balancer (ALB) that performs the redirection.

This rule can be configured to inspect incoming requests and redirect them to HTTPS if they are received over HTTP.

By configuring this rule, you can ensure that all requests to your website are securely handled over HTTPS.

Question 18

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes.

What should a solutions architect do to accomplish this goal?

A. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).

B. Turn on AWS Config with the appropriate rules. **Correct answer**

C. Turn on Amazon Inspector with the appropriate assessment template.

D. Turn on AWS Trusted Advisor with the appropriate checks.

Overall explanation
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to monitor and record changes to the configuration of your Amazon S3 buckets.

By turning on AWS Config and enabling the appropriate rules, you can ensure that your S3 buckets do not have unauthorized configuration changes.

Question 19

A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.

What should a solutions architect do to meet these requirements?

A. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions. **Correct answer**

B. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.

C. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.

D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

Overall explanation
Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.

Explanation:

Amazon Rekognition is a service that offers pre-trained machine learning models for image and video analysis, including detecting inappropriate content. It can quickly and accurately detect explicit or suggestive content within images.

For low-confidence predictions, you can set up a human review workflow through Amazon Rekognition Custom Labels. This allows human reviewers to review and confirm the inappropriate content, thus reducing the chances of false positives or negatives.

Using Amazon Rekognition for inappropriate content detection minimizes the development effort compared to building a custom machine learning model and is a cost-effective way to ensure content moderation on your social media website.

Question 20

A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53.
What should a solutions architect do to meet these requirements?

A. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content. Point the other domain name to the accelerator DNS name for static content. Use the domain names as endpoints for the web application.

B. Create an Amazon CloudFront distribution that has the S3 bucket as an origin. Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints. Create a custom domain name that points to the accelerator DNS name. Use the custom domain name as an endpoint for the web application.**Correct answer**

C. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.

D. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint Configure Route 53 to route traffic to the CloudFront distribution.

Overall explanation

Create an Amazon CloudFront distribution that has the S3 bucket as an origin to accelerate the static content.

Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints.

Create a custom domain name that points to the accelerator DNS name.

Use the custom domain name as an endpoint for the web application.

Question 21

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 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.**Correct answer**

B. 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.

C. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.

D. 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.

Overall explanation

Using AWS Fargate allows you to run containers without managing the underlying infrastructure. Using ECS with Fargate for the scheduled task minimizes operational overhead.

Question 22

A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources.

What should a solutions architect do to meet these requirements?

A. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.**Correct answer**

B. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.

C. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.

D. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls.

Overall explanation
AWS Config is specifically designed to track and record configuration changes on AWS resources. It provides historical data on the state of your resources and allows you to evaluate changes over time.

On the other hand, AWS CloudTrail is designed to record API calls made on your AWS account, providing an audit trail for actions taken via the AWS Management Console, AWS CLI, SDKs, etc.

This combination allows you to meet compliance, governance, auditing, and security requirements effectively.

Question 23

A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically. is highly available, and requires minimum operational overhead.

Which solution will meet these requirements?

A. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.**Correct answer**

B. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

D. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.

Overall explanation

Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group and use Amazon Elastic File System (Amazon EFS) for storage.

Here's why this is a suitable choice:

Scalability: Amazon EFS can scale automatically as your storage needs grow, and it can handle varying file sizes efficiently.

High Availability: Multi-AZ deployment ensures high availability by replicating data across multiple Availability Zones, making it resilient to failures.

Standard File System Structure: Amazon EFS provides an NFS-based file system, which offers a standard file system structure that can be easily used by applications.

Minimum Operational Overhead: As a managed service, Amazon EFS abstracts much of the operational overhead, like hardware provisioning and maintenance, from you.

Ease of Integration: Amazon EFS is easily integrated with Amazon EC2 instances, making it a seamless choice for migrating your application.

While running containers with Amazon ECS or Amazon EKS could be an option, using Amazon EFS simplifies the storage aspect and meets the requirement of a standard file system structure. Running on EC2 instances with Amazon EFS provides a simple and highly available solution with minimal operational overhead for file storage.

Question 24

A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

A. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

B. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.

C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.

D. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select. **Correct answer**

Overall explanation
Amazon S3 Intelligent-Tiering: This storage class is designed to optimize costs for data with unknown or changing access patterns. It automatically moves objects between two access tiers: frequent and infrequent access. In your case, this is suitable

for the files that are accessed within the first year (frequent access) and the ones accessed less frequently after 1 year (infrequent access).

Amazon Athena for Querying: You can use Amazon Athena, an interactive query service, to query and retrieve the files that are still stored in the S3 Intelligent-Tiering access tiers. This allows you to quickly access files that are less than 1 year old.

S3 Glacier Select for Retrieval: For the files that have transitioned to S3 Glacier (after 1 year), you can use S3 Glacier Select to retrieve specific data from the archives without having to restore the entire object. This provides a cost-effective retrieval mechanism for older files.

Question 25

An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours.

Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones. Add an Application Load Balancer (ALB) to distribute the website traffic. Add another ALB for the backend APIs. Store the data in Amazon RDS for MySQL.

B. Use Amazon S3 to host the full website in different S3 buckets. Add Amazon CloudFront distributions. Set the S3 buckets as origins for the distributions. Store the order data in Amazon S3.

C. Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.**Correct answer**

D. Migrate the full application to run in containers. Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic. Store the data in Amazon RDS for MySQL.

Overall explanation
Scalability: Amazon S3 and Amazon CloudFront are highly scalable and can handle millions of requests with low latency. Amazon S3 is great for hosting static content, and CloudFront provides a content delivery network (CDN) to cache content close to end-users.

Serverless Backend: Using Amazon API Gateway and AWS Lambda for the backend APIs provides serverless architecture, eliminating the operational overhead of managing servers. AWS Lambda can automatically scale based on the incoming traffic, making it cost-effective and efficient.

Database: Amazon DynamoDB is a highly scalable NoSQL database that can handle the required throughput. It's designed for low-latency, high-performance applications and can scale as needed.

Question 26

A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.

What should the solutions architect do to meet these requirements?

A. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.

B. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.

C. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an Auto Scaling group.

D. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.**Correct answer**

Overall explanation
Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.

Explanation:

Elastic Beanstalk: Elastic Beanstalk simplifies the deployment and management of applications, including Java applications running on Apache Tomcat.

Load-Balanced Environment: Configuring a load-balanced environment ensures high availability and distribution of incoming traffic among multiple instances.

Rolling Deployment Policy: Elastic Beanstalk supports rolling deployments, minimizing downtime during application updates by gradually replacing instances.

Managed Environment: Elastic Beanstalk provides a managed environment, handling capacity provisioning, load balancing, and automatic scaling.

Efficient Deployment: Rolling deployments ensure efficient and reliable application updates without disrupting the availability of the application.

Question 27

A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.
How should a solutions architect design the architecture to meet these requirements?

A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.

B. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.

C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.**Correct answer**

D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.

Overall explanation
Amazon SQS for Decoupling: Using Amazon SQS to queue jobs is a common and effective approach for decoupling components in a distributed application. It ensures that the primary server doesn't have to be directly connected to the compute nodes, which allows for better scalability and fault tolerance.

Auto Scaling based on Queue Size: By configuring EC2 Auto Scaling based on the size of the SQS queue, you can automatically adjust the number of compute nodes according to the incoming workload. This approach ensures that you scale your compute nodes dynamically in response to the workload, which aligns with the requirements for resiliency and scalability.

Question 28

A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege.

Which solution will meet these requirements?

A. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

B. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.

C. Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.**Correct answer**

D. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.

Overall explanation

IAM User: By creating an IAM user, you can grant the product manager specific and limited permissions for accessing CloudWatch, in this case, read-only access.

Least Privilege: Attaching the CloudWatchReadOnlyAccess AWS managed policy ensures that the product manager has the minimum required permissions to view the dashboard, aligning with the principle of least privilege.

Login Credentials: Providing the product manager with their own login credentials ensures accountability and auditability.

Dashboard URL: Sharing the URL of the specific dashboard allows the product manager to access it directly without navigating through the AWS Management Console, making it more user-friendly.

Question 29

A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.

Which solution will meet these requirements?

A. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

B. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.

C. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.**Correct answer**

D. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

Overall explanation

AWS Single Sign-On (AWS SSO): AWS SSO is an identity management service provided by Amazon Web Services. It allows you to centrally manage SSO access to multiple AWS accounts and applications. With AWS SSO, you can create and manage users, grant permissions to AWS accounts, and configure SSO settings.

Two-Way Forest Trust: In this context, a "forest" refers to a collection of one or more Active Directory domains that share a common schema. A trust is a relationship established between domains or forests to allow users in one domain to access resources in another.

Connecting with AWS SSO: To enable SSO access to AWS accounts from your company's self-managed Microsoft Active Directory, you create a two-way trust between the on-premises AD forest and AWS SSO.

Here's a more detailed explanation of the steps involved:

Enable AWS SSO: From the AWS SSO console, you enable AWS SSO. This sets up the SSO service within your AWS environment.

Create a Two-Way Forest Trust: You establish a two-way trust relationship between your on-premises Active Directory forest and AWS SSO. This trust relationship allows user authentication and authorization between your on-premises AD and AWS SSO.

Sync Users and Groups: AWS SSO allows you to synchronize users and groups from your on-premises AD into AWS SSO. This means that your existing users and groups in your self-managed AD can be used for access to AWS resources.

Grant Access to AWS Accounts: Once your users and groups are synchronized, you can grant them access to your AWS accounts and applications, providing the necessary permissions.

Single Sign-On: Users can then log in to their AWS accounts and applications using their on-premises AD credentials without the need for separate AWS-specific usernames and passwords.

The two-way trust allows users to authenticate and access AWS services using their existing on-premises credentials. This approach simplifies user management and access control across both your on-premises environment and AWS, making it a suitable solution for organizations that want to maintain a single source of user identity and credentials while using AWS services.

Question 30

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.**Correct answer**

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. 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.

D. 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.

Overall explanation

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.

Explanation:

Deploying the application servers across multiple Availability Zones (AZs) in an Auto Scaling group ensures high availability and avoids single points of failure.

Using Amazon RDS with Multi-AZ configuration for the database provides automatic failover in the event of a failure in the primary database instance, enhancing resilience.

This architecture supports scalability by utilizing Auto Scaling for the application servers, allowing them to scale based on demand.

The Multi-AZ configuration for RDS also enhances data durability by maintaining synchronous copies of the database in different AZs.

Overall, this solution meets the requirements of high availability, resilience, and scalability.

Question 31

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 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.

C. 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.

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. **Correct answer**

Overall explanation
Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Explanation:
Amazon FSx for Lustre is a fully managed, high-performance file system that can be used to support Lustre clients.

It provides durability, high throughput, and low latency for applications that require fast access to shared data.

Using FSx for Lustre is the recommended solution for fully managed shared storage with Lustre client support.

Question 32

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 Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

B. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.

C. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.**Correct answer**

D. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

Overall explanation

Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.

Explanation:

Reserved Instances (RIs): RIs provide significant cost savings for predictable workloads with frontend nodes running 24/7.

Spot Instances: Spot Instances are cost-effective for variable and short-lived workloads, making them suitable for backend nodes with varying demand.

Frontend Nodes Stability: Using RIs for frontend nodes ensures stable, continuous availability without interruption.

Backend Nodes Cost-Effective Scaling: Spot Instances allow cost-effective scaling for backend nodes, meeting the varying workload requirements.

Cost Optimization: This combination provides a cost-effective solution by leveraging RIs for stability and Spot Instances for scalability.

Question 33

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 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.**Correct answer**

D. 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.

Overall explanation
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.

Explanation:
S3 Block Public Access: Enabling this feature on the account level ensures that no S3 objects in any bucket can be made public.

AWS Organizations SCP: A service control policy (SCP) in AWS Organizations allows you to set fine-grained permissions and restrictions across accounts.

Preventing Changes: By creating an SCP that restricts the modification of S3 Block Public Access settings, you enforce the least privilege principle.

Automation: Using SCPs helps automate and centrally manage access policies across multiple accounts.

Compliance with Security Policy: This solution aligns with the security policy of keeping all S3 objects private.

Question 34

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. Create a signed request using the existing IAM credentials in the Lambda function.

B. Create a new IAM user and use the existing IAM credentials in the Lambda function.

C. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.**Correct answer**

D. Add required IAM permissions in the resource policy of the Lambda function.

Overall explanation
Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

Explanation:

Lambda functions require execution roles to grant permissions to access AWS services.

Creating an IAM execution role with the necessary permissions for S3 access and attaching it to the Lambda function ensures that the function has the required permissions to upload files to S3.

The IAM user credentials are not used directly within the Lambda function; instead, an IAM role is assumed.

Question 35

A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

A. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

B. Stop the DB instance when tests are completed. Restart the DB instance when required.

C. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.

D. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.**Correct answer**

Overall explanation
Cost Efficiency: By terminating the DB instance when not in use, you eliminate the ongoing costs associated with running the RDS instance. You only incur costs for the storage of the snapshot, which is typically less expensive than running a full RDS instance.

Isolation: Terminating the instance provides isolation between the resource-intensive testing period and regular operation. This ensures that the tests don't impact the performance or resource availability of the database during normal operations.

Quick Recovery: Restoring the database from a snapshot is a relatively quick process. It allows you to quickly prepare and set up the RDS instance in the desired state for testing when needed.

Question 36

A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability.
Which solution meets these requirements?

A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.

B. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SOS) subscriptions. Configure the consumer applications to process the messages from the queues.**Correct answer**

C. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.

D. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.

Overall explanation
Decoupling and Scalability: Amazon SNS and Amazon SQS are designed for decoupling and scaling applications. SNS allows you to publish messages to topics, and subscribers can receive those messages asynchronously. By using multiple SQS subscriptions to an SNS topic, you can ensure that multiple consumer applications can independently process the messages at their own rates.

Handling Varying Message Rates: SNS and SQS can efficiently handle varying message rates. As the number of incoming messages fluctuates, AWS automatically scales SQS and the consumer applications as needed. This ensures that the system can handle sudden increases in the message rate, such as 100,000 messages per second.

Reliability and Durability: Amazon SQS provides message durability and reliability. Messages are stored redundantly, and the system is designed to ensure that messages are not lost in transit. This is crucial for handling a high volume of messages.

Question 37

A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.**Correct answer**

B. Create an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.

C. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

D. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.

Overall explanation
Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.

With this approach, you create a single customer managed KMS key that's available in multiple AWS Regions. This key can be used to encrypt and decrypt data in both Regions consistently. You then configure S3 buckets in each Region to use server-side encryption with AWS KMS keys (SSE-KMS) and associate them with this multi-Region KMS key. Configuring replication between the S3 buckets ensures that data is synchronized between the two Regions.

Client-side encryption would involve the application itself handling encryption, which may require more operational overhead compared to using server-side encryption with KMS keys. This approach also aligns with the requirement of using the same KMS key for encryption and decryption in both Regions.

Question 38

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. 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.**Correct answer**

C. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS 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.

Overall explanation

Since the application has no local data on instances, AMIs alone can meet the RPO by restoring instances from the most recent AMI backup. When combined with automated RDS backups for the database, this provides a complete backup solution for this environment.

The other options involving EBS snapshots would be unnecessary given the stateless nature of the instances. AMIs provide all the backup needed for the app tier. This uses native, automated AWS backup features that require minimal ongoing management: - AMI automated backups provide point-in-time recovery for the stateless app tier. - RDS automated backups provide point-in-time recovery for the database.

Question 39

A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a

third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.
A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server.

Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

B. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.**Correct answer**

C. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.

D. Deploy a transit gateway in the inspection VPConfigure route tables to route the incoming packets through the transit gateway.

Overall explanation
Network Load Balancer (NLB): NLB is designed for high availability and ultra-low latency at the transport layer (Layer 4). It's a suitable choice for routing traffic to the appliance for packet inspection without much overhead.

Least Operational Overhead: NLB is a simple and straightforward solution for routing traffic to the appliance. It doesn't introduce additional complexity compared to some of the other options.

Question 40

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 AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.

B. 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.

C. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.

D. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.**Correct answer**

Overall explanation
Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.

Explanation:
Creating EBS volumes as encrypted volumes ensures that all data written to those volumes is encrypted at rest. This provides data security for the application running on EC2 instances.

Question 41

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

A. Create an Amazon S3 bucket and host the website there.**Correct answer**

B. Containerize the website and host it in AWS Fargate.

C. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

D. Deploy a web server on an Amazon EC2 instance to host the website.

Overall explanation
This is the most cost-effective option for hosting a simple static website consisting of HTML, CSS, client-side JavaScript, and images. Amazon S3 is designed for scalable and cost-effective storage of objects, making it ideal for serving static content like a website.

You can configure the S3 bucket to act as a static website host, and it can serve your website content directly to users without the need for additional servers or containers. It's a simple and efficient way to host static content while keeping costs low.

Question 42

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. Create a read replica for the RDS DB instance.**Correct answer**

C. Configure a Multi-AZ deployment for the RDS DB instance.

D. Set up an Amazon CloudFront distribution.**Correct answer**

E. Host the dynamic web content in Amazon S3.

Overall explanation
Set up an Amazon CloudFront distribution.

Create a read replica for the RDS DB instance.

Explanation:

Amazon CloudFront: Distributing static content through CloudFront accelerates page loads by caching content at edge locations globally, reducing latency.

Read Replicas: Creating read replicas for the RDS DB instance offloads read operations, improving overall database performance.

Global Content Delivery: CloudFront's global network ensures faster content delivery to users around the world, enhancing the user experience.

Optimizing Database Load: Read replicas distribute read traffic, preventing the primary database from being overloaded, especially during peak times.

Scalability: Both CloudFront and RDS read replicas contribute to improved scalability and performance of the web application.

Question 43

A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.

Which solution meets these requirements MOST cost-effectively?

A. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

B. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

C. Save the .pdf files to Amazon DynamoDUse the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.

D. Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.**Correct answer**

Overall explanation
Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.

Explanation:

This solution is the most cost-effective and scalable among the provided options. It leverages Amazon S3 for storage, which is highly scalable, durable, and designed for object storage.

Using S3 PUT events to trigger an AWS Lambda function for conversion allows for a serverless, event-driven architecture that can automatically scale based on demand.

AWS Lambda scales automatically, and you only pay for the compute resources used during execution.

Question 44

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture.

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.

B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.

C. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

D. Use Amazon Athena directly with Amazon S3 to run the queries as needed.**Correct answer**

Overall explanation

Minimal Operational Overhead: Amazon Athena is a serverless query service that allows you to run SQL queries directly on data stored in Amazon S3. There is no need to provision or manage servers, clusters, or infrastructure. This significantly reduces operational overhead, as you only need to focus on running your queries.

Simple Integration: Amazon Athena seamlessly integrates with data stored in Amazon S3, including JSON-formatted data. There's no need to move or transform the data, making it the most straightforward solution for analyzing log files with minimal architectural changes.

On-Demand Queries: Amazon Athena allows you to run queries on-demand. You only pay for the queries you execute, which is cost-effective and aligns well with your simple, on-demand query requirements.

Support for SQL Queries: Amazon Athena supports standard SQL queries, making it easy to write and execute the queries needed for log file analysis.

Question 45

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an

Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

A. Configure the Application Load Balancer to direct a user to the server with the documents

B. Copy the data so both EBS volumes contain all the documents

C. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

D. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.**Correct answer**

Overall explanation
Data Consistency: Amazon EFS is a managed file storage service that provides a shared, scalable file system accessible from multiple EC2 instances. By copying the data from both EBS volumes to Amazon EFS, you ensure that both EC2 instances have access to the same set of documents. This eliminates the issue of users seeing different subsets of their documents.

Scalability and Availability: Amazon EFS is designed for high availability and can be mounted by multiple EC2 instances across different Availability Zones. This aligns with your goal of better scalability and availability.

Real-Time Data Access: By saving new documents to Amazon EFS, you ensure that any newly uploaded documents are immediately accessible to both EC2 instances. This is crucial for maintaining data consistency and ensuring users can see all their documents at once.

Question 46
A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and

there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.
Which solution meets these requirements?

A. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

B. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.

C. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.**Correct answer**

D. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.

Overall explanation
AWS Direct Connect provides a dedicated network connection from your on-premises data center to AWS. It offers a more reliable and higher bandwidth connection compared to typical internet connections.

By establishing a new AWS Direct Connect connection specifically for the backup traffic, you can ensure that backups are sent to Amazon S3 with minimal impact on your internet connectivity for internal users. This allows you to take advantage of the dedicated network connection for your backup needs.

AWS Snowball (option D) is not ideal for time-sensitive data since it involves manual data transfer and shipping, which may not provide the required speed for timely backups.

Submitting a support ticket (option A) is not a solution to address bandwidth limitations, and AWS service limits do not apply to this scenario.

Question 47
A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances. Amazon RDS DB instances. and Amazon Redshift clusters are configured

with tags. The company wants to minimize the effort of configuring and operating this check.

What should a solutions architect do to accomplish this?

A. Use AWS Config rules to define and detect resources that are not properly tagged.**Correct answer**

B. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.

C. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

D. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.

Overall explanation

AWS Config rules are designed to help assess and monitor the configuration of AWS resources, including their tag compliance. By creating a custom AWS Config rule, you can define the tagging requirements for your Amazon EC2 instances, RDS DB instances, and Redshift clusters.

This rule can check whether the necessary tags are present and properly allocated to these resources. If a resource is found to be non-compliant with the tagging requirements, AWS Config can automatically flag it, allowing you to take corrective actions.

This approach is more automated and requires less manual effort compared to options **B, C,** and **D.** With AWS Config, you can continuously monitor and enforce tagging standards without the need for manual checks or custom code. Additionally, AWS Config offers real-time visibility into your resource compliance status.

Question 48

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.

During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.

Which solution will meet these requirements?

A. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

B. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).

C. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.

D. Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.**Correct answer**

Overall explanation
Scalability: Amazon DynamoDB is a fully managed NoSQL database service designed for high scalability and performance. DynamoDB can easily handle high volumes of data and automatically scales to accommodate increased workloads.

DynamoDB Accelerator (DAX): DAX is an in-memory caching service that can significantly improve the read performance of DynamoDB tables. It helps reduce the database load and latency, making it a suitable choice for handling high volumes of data.

Minimized Configuration Effort: By choosing DynamoDB with DAX, you can continue using the existing DynamoDB API calls without significant changes to your application. This minimizes configuration effort and simplifies the migration process.

Question 49
An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.
Which solution will provide private network connectivity to Amazon S3?

A. Create a gateway VPC endpoint to the S3 bucket.**Correct answer**

B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.

C. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

D. Create an instance profile on Amazon EC2 to allow S3 access.

Overall explanation
VPC Endpoint for S3: Amazon VPC Endpoints enable you to privately connect your VPC to supported AWS services, including Amazon S3, without requiring internet access. This means your EC2 instance can securely access S3 resources within the same VPC.

Isolation from the Internet: With a VPC endpoint, you ensure that your application running on the EC2 instance can access S3 without being exposed to the public internet. This enhances security and reduces the risk of potential security threats.

Question 50
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. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.

B. Create a user in the production account with unique credentials for each team member.

C. Add the development account as a principal in the trust policy of the role in the production account.**Correct answer**

D. Attach the Administrator Access policy to the development account users.

Overall explanation
Add the development account as a principal in the trust policy of the role in the production account.

Explanation:
Cross-Account Access: Adding the development account as a principal in the trust policy enables cross-account access to the IAM role in the production account.

IAM Role Trust Policy: This approach adheres to the principle of least privilege by explicitly specifying the trusted account for access.

Avoiding Unique Credentials: Rather than creating additional IAM users in the production account, leveraging IAM roles promotes better security practices.

Scalability: This solution scales efficiently as team members from the development account can assume the role without requiring individual IAM users.

Centralized Management: IAM roles provide centralized management of permissions, making it easier to control access across multiple AWS accounts.

Question 51
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. Organization

B. Amazon Elastic Container Service (Amazon ECS) resource

C. Role **Correct answer**

D. Amazon EC2 resource

E. Group **Correct answer**

Overall explanation
Identity-based policy used for role and group

Explanation:
Role: IAM roles are entities with policies that determine what actions can be performed on what resources. Roles can be assumed by IAM users, AWS services, or AWS resources.

Group: IAM groups are containers for IAM users. Policies attached to groups apply to all users in the group, simplifying permission management.

IAM Policy: The provided policy can be attached to both IAM roles and IAM groups, allowing for flexible and reusable permission management.

Resource-Specific Permissions: The policy grants specific permissions related to EC2 actions within the us-east-1 Region.

Policy Conditions: The policy includes a condition that requires multi-factor authentication (MFA) for certain EC2 actions, enhancing security.

Question 52
A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved Instances that specify the Region needed.

B. Create an On-Demand Capacity Reservation that specifies the Region needed.

C. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.**Correct answer**

D. Purchase Reserved Instances that specify the Region and three Availability Zones needed.

Overall explanation
Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

This ensures that the company has reserved capacity in the desired Region and Availability Zones for the specified duration without having to make an upfront payment as is the case with Reserved Instances.

On-Demand Capacity Reservations provide greater flexibility for short-term capacity requirements, such as events or peak workloads.

Question 53
A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

A. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.

B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

C. Configure S3 Intelligent-Tiering to automatically migrate objects.

D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.**Correct answer**

Overall explanation
Amazon S3 Glacier Deep Archive is a secure, durable, and extremely low-cost Amazon S3 storage class for long-term retention of data that is rarely accessed and for which retrieval times of several hours are acceptable. It is the lowest-cost storage option in Amazon S3, making it a cost-effective choice for storing backup files that are not accessed after 1 month.

Question 54
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. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).**Correct answer**

B. Create a separate application tier using EC2 instances dedicated to email processing.

C. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

D. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).

Overall explanation
Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).

Explanation:
Offload Email Processing: Configuring the web instance to send emails through Amazon SES offloads the email processing workload from the application servers, reducing latency.

Amazon SES Benefits: SES is a fully managed email service that ensures high deliverability, scalability, and reliability of email communication.

Minimize Operational Overhead: Utilizing Amazon SES reduces the operational overhead associated with managing a dedicated email processing tier.

Cost-Effective: Amazon SES provides a cost-effective solution for sending emails, especially when compared to managing a separate EC2-based email processing tier.

Scalability: Amazon SES can easily handle the increasing volume of emails as the application's user traffic grows.

Question 55
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 a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.

B. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.

C. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.**Correct answer**

D. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.

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.**Correct answer**

Overall explanation

AWS Auto Scaling can dynamically adjust the capacity of the Application Load Balancer (ALB) based on the request rate, ensuring that the system can scale to meet demand during working hours.

Using scheduled scaling to set Auto Scaling group capacity to zero during weekends helps save costs by minimizing resources when the system doesn't require high availability.

Question 56

A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.

C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.**Correct answer**

D. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.

Overall explanation

Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Explanation:
Amazon Textract is a service designed for extracting text and data from documents, which includes PDF and JPEG files. It can accurately extract text and helps identify key information.

Amazon Comprehend Medical is specifically designed for identifying protected health information (PHI) within text, making it a suitable choice for healthcare-related applications.

Using these two services, you can offload the heavy lifting of text extraction and PHI identification to AWS-managed services, reducing operational overhead and ensuring accurate results for healthcare data analysis.

Question 57
A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.
Which solution will meet these requirements?

A. Create an S3 bucket. Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.

B. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

C. Set up an AWS Direct Connect connection between the on-premises network and AWS. Deploy an S3 File Gateway on premises. Create a public virtual interface (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

D. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.**Correct answer**

Overall explanation
Minimizing Network Bandwidth: AWS Snowball Edge is designed for high-volume data migration and is an ideal solution for situations where minimizing network bandwidth is a primary concern. You can transfer the data to the Snowball Edge device on premises, which does not consume your internet bandwidth.

Large Data Volumes: Snowball Edge is built for large data sets, and it supports a wide range of data sizes, including the video files ranging from 1 MB to 500 GB. It can handle the 70 TB of data efficiently.

Convenient Data Transfer: With Snowball Edge, you don't need to rely on internet speed or face data transfer challenges, which is often the case when copying data directly to S3 over the internet.

Security: Snowball Edge devices are highly secure and tamper-evident, ensuring the safety of your data during transit.

Question 58
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. 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.

C. 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.

D. 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.**Correct answer**

Overall explanation
Amazon Transcribe supports PII redaction, and you can configure transcription jobs with redaction features.

Using Amazon Transcribe, combined with Lambda for automation, allows for the extraction of text from audio files with PII redaction.

Question 59
An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.
A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Choose two.)

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.**Correct answer**

B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.**Correct answer**

C. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.

D. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon ample Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

E. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.

Overall explanation

Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.

This sets up an SQS queue to receive notifications when an image is uploaded to the S3 bucket, allowing for event-driven processing.

Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.

This configures AWS Lambda to be triggered by messages in the SQS queue, ensuring that each image upload triggers the Lambda function for processing. Deleting the message after successful processing helps ensure that messages are not processed more than once.

Question 60

A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.

Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Enable versioning on the S3 bucket.**Correct answer**

B. Enable MFA Delete on the S3 bucket.**Correct answer**

C. Enable default encryption on the S3 bucket.

D. Create a bucket policy on the S3 bucket.

E. Create a lifecycle policy for the objects in the S3 bucket.

Overall explanation
Enable versioning on the S3 bucket.

Versioning keeps multiple versions of an object in the same S3 bucket. If an object is deleted, the previous versions can still be accessed, preventing accidental data loss.

Enable MFA Delete on the S3 bucket.

Multi-Factor Authentication (MFA) Delete requires additional authentication (in the form of an MFA device) for the deletion of objects. This provides an extra layer of protection against accidental deletions.

Question 61
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.

Which solution will meet these requirements with the LEAST operational overhead?

A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.

B. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.**Correct answer**

C. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.

D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store. Turn on automatic rotation for the encrypted parameters. Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Overall explanation

Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

Explanation:

AWS Secrets Manager is designed for storing, managing, and rotating sensitive information like database credentials. When you use AWS Secrets Manager, you can enable automatic rotation of the credentials, which is a best practice for security.

This rotation can be managed seamlessly without the need for manual intervention. By attaching the necessary permissions to the EC2 instance's role, your application can securely retrieve the credentials from AWS Secrets Manager, ensuring that the credentials are not hardcoded in the application and that they are automatically rotated. This approach minimizes operational overhead and provides a highly secure and automated solution.

Question 62

A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.
The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.
Which solution meets these requirements?

A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.**Correct answer**

B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.

C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.

D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Overall explanation

1. S3 Transfer Acceleration Benefit: Enabling S3 Transfer Acceleration provides an efficient method to accelerate data uploads to your S3 bucket. This is achieved by utilizing Amazon's Content Delivery Network (CDN) to optimize the transfer path.

2. High-Speed Internet Connections: Given that each site has a high-speed Internet connection, this choice aligns well with the capability to transfer data quickly. The combination of Transfer Acceleration and high-speed connections can significantly enhance the upload performance.

3. Reduced Latency: Transfer Acceleration minimizes the effects of network latency, allowing data to be uploaded more rapidly. It's particularly advantageous when dealing with distant or geographically dispersed sites.

4. Minimized Operational Complexity: This approach keeps things simple. It directly uploads data to the destination S3 bucket, which means there's no need for additional services or configurations that might introduce complexity.

5. Direct Path to Destination: Data is sent directly to the destination bucket, eliminating the need for intermediate steps, such as copying data between S3 buckets, that can slow down the process.

6. Cost-Efficient: While there might be some additional costs associated with using Transfer Acceleration, this approach can be cost-effective compared to other methods that involve data replication or specialized hardware devices.

7. Real-Time Data Availability: Data is available in near real-time in the destination bucket, as there's no need to wait for replication or data transfer jobs to complete. This is crucial for applications or processes that require immediate access to the latest data.

8. Simplified Maintenance: With a straightforward data transfer process, you can minimize the need for ongoing maintenance and monitoring. This helps keep the solution easy to manage.

It's important to consider potential costs, security measures, and data redundancy requirements in your decision-making process. While Option A can provide a fast and straightforward data transfer, make sure it aligns with your specific needs and constraints before implementing it.

Question 63
A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.
Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.

What should a solutions architect do to meet these requirements with the LEAST development effort?

A. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.

B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII. **Correct answer**

C. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.

D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the meats that contain PII.

Overall explanation
Amazon Macie: Amazon Macie is a machine learning service that helps discover, classify, and protect sensitive data, including PII, in Amazon S3 buckets. By using Macie, you can automatically scan the objects for PII without having to develop custom scanning algorithms. It simplifies the detection process.

Amazon SNS: Amazon SNS can be used to send notifications to administrators when PII is detected in the objects. This is an efficient way to alert administrators about the issue.

Manual remediation: This approach involves administrators manually removing the objects that contain PII. This is usually preferred in situations where you want human intervention to ensure the accuracy of the decision to remove such data.

Question 64
A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability.

What should a solutions architect do to meet these requirements?

A. Create an AWS Lambda function to apply the patch to all EC2 instances.

B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.**Correct answer**

C. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

D. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.

Overall explanation
AWS Systems Manager Patch Manager is a fully managed service that automates the process of patching and managing software across your Amazon EC2 instances. It is specifically designed for tasks like this where you need to apply patches to a large number of instances.

With AWS Systems Manager Patch Manager, you can define patch baselines, schedule maintenance windows, and quickly apply patches to EC2 instances. It provides you with a centralized and efficient way to keep your instances up-to-date with security patches.

Running custom scripts (option D) or using AWS Lambda functions (option A) to patch instances can be more complex and less efficient for handling large-scale patching, especially in a time-critical security scenario. Systems Manager Patch Manager simplifies and automates the process.

Question 65
A serverless application uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The Lambda function needs permissions to read and write to the DynamoDB table.

Which solution will give the Lambda function access to the DynamoDB table MOST securely?

A. Create an IAM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.

B. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.

C. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration.

D. Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.**Correct answer**

Overall explanation
Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.

Explanation:
IAM Role: Creating an IAM role allows fine-grained control over permissions, and Lambda functions can assume roles for access to AWS resources.

Policy for DynamoDB Access: Attaching a policy to the role that grants read and write access to the DynamoDB table ensures the Lambda function has the necessary permissions.

Trusted Service: Including Lambda as a trusted service in the IAM role allows the Lambda function to assume the role.

Dynamic Permissions: The IAM role approach ensures that permissions are dynamically assigned to the Lambda function, enhancing security.

Least Privilege: This solution adheres to the principle of least privilege by granting only the necessary permissions for DynamoDB access.

Question 66
A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

A. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.**Correct answer**

B. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

C. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.

D. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.**Correct answer**

E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.

Overall explanation
Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Explanation:
AWS Lambda for File Conversion: Using Lambda for converting .csv files into images ensures a serverless, scalable, and cost-effective solution.

Event-Driven Execution: Lambda can be triggered by S3 events, ensuring automatic execution when a .csv file is uploaded.

S3 Lifecycle Rules: Lifecycle rules are applied to both .csv files and image files, allowing for efficient management of storage costs.

Transition to S3 Standard-IA: Transitioning .csv files to S3 Standard-IA after 1 day optimizes storage costs based on access patterns.

Reduced Redundancy Storage (RRS): Storing image files in RRS may be cost-effective, considering the images become irrelevant after 30 days.

This combination provides a cost-effective, scalable, and well-architected solution for the given requirements.

Question 67
A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

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

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

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

D. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.**Correct answer**

Overall explanation
IAM Roles: IAM roles are designed for granting temporary permissions to AWS services, such as EC2 instances. Roles provide secure and efficient access to AWS resources without the need for long-term credentials like access keys.

Least Privilege: IAM roles can be set up with the principle of least privilege, meaning you can define specific permissions for the role to access the S3 bucket without granting unnecessary or overly permissive permissions.

Question 68
A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.
The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.
Which solution will meet these requirements?

A. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

B. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.**Correct answer**

C. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.

D. Use Amazon Redshift with a single node for leader and compute functionality.

Overall explanation
Amazon Aurora: Amazon Aurora is a high-performance, fully managed database service that is compatible with MySQL and provides excellent read scaling capabilities.

Multi-AZ Deployment: Aurora supports a Multi-AZ deployment, which ensures high availability and automatic failover in case of an issue with the primary instance. This is important for maintaining high availability.

Aurora Auto Scaling: Aurora allows you to configure Auto Scaling with Aurora Replicas. With Aurora Auto Scaling, you can automatically add read replicas in response to increased read demand, and these replicas can help distribute the read workload, improving performance.

Question 69
A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

A. Enable Amazon Inspector on the EC2 instances.

B. Enable AWS Shield Advanced and assign the ELB to it.**Correct answer**

C. Enable AWS Shield and assign Amazon Route 53 to it.

D. Enable Amazon GuardDuty on the account.

Overall explanation
AWS Shield Advanced is a managed Distributed Denial of Service (DDoS) protection service that provides additional protection beyond what is provided by AWS Shield Standard.

It's designed to protect against larger and more sophisticated DDoS attacks. By assigning the Elastic Load Balancer (ELB) to AWS Shield Advanced, you can leverage its protection capabilities and guard against large-scale DDoS attacks.

This is an effective solution for public-facing web applications where DDoS protection is essential.

Question 70
A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.
A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

A. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.

B. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.**Correct answer**

C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.

D. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.

Overall explanation

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation.

This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

Question 71

A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.

Which solution will meet these requirements?

A. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.

C. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.**Correct answer**

D. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

Overall explanation
Amazon QuickSight: Amazon QuickSight is a fully managed, serverless business intelligence service that makes it easy to create interactive visualizations and reports. It is designed for data visualization and reporting.

Fine-Grained Access Control: Amazon QuickSight allows you to create fine-grained access controls, allowing you to share dashboards and visualizations with specific users and groups, granting them access to only the data and insights they need.

Question 72
A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet these requirements?

A. Use Amazon EC2 instances, and install Docker on the instances.

B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.

C. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.**Correct answer**

Overall explanation
Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

Explanation:

Amazon ECS on AWS Fargate is a serverless container management service. With Fargate, you don't need to provision or manage the underlying infrastructure (Amazon EC2 instances).

It allows you to focus on running your containerized applications while AWS takes care of the infrastructure management.

This is an ideal choice when you want to run containerized workloads without the operational overhead of managing the underlying EC2 instances, making it a suitable option for companies that prefer to focus on maintaining their critical applications.

Question 73
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 Organizations management account, specify the Default EBS volume encryption setting.**Correct answer**

B. Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action whenthe ec2:Encrypted condition equals false.**Correct answer**

C. Update the IAM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.

D. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.

E. 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.

Overall explanation
Creating an SCP and attaching it to the root organizational unit (OU) will deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false. This means that any IAM user or root user in any account in the organization will not be able to create an EBS volume without encrypting it.

Specifying the Default EBS volume encryption setting in the Organizations management account will ensure that all new EBS volumes created in any account in the organization are encrypted by default.

Question 74
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. Increase the number of IOPS on the gp3 volume.

B. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

C. Replace the volume with a magnetic volume.

D. Replace the volume with a Provisioned IOPS SSD (io2) volume.**Correct answer**

Overall explanation
The performance issue with the gp3 volume suggests a need for higher IOPS. The io2 volume type is designed for critical database workloads that require sustained high IOPS performance.

Question 75
A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

A. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.

C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.

D. Add the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.**Correct answer**

Overall explanation
Simple and Direct Approach: Adding the aws PrincipalOrgID condition key directly in the S3 bucket policy is a straightforward way to restrict access to users from accounts

within the AWS Organization. It requires minimal configuration and ongoing management.

Organization-Wide Restriction: By specifying the organization's ID as the condition, you ensure that only users from accounts within the organization can access the S3 bucket. This directly aligns with the requirement of limiting access to the organization's users.

Question 76
A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.

Which solution will meet these requirements?

A. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.**Correct answer**

B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.

C. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

D. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.

Overall explanation
Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.

Explanation:

By creating a security group (SG) for the RDS instances and allowing inbound traffic from the security group assigned to the EC2 instances in the private subnets, you control and restrict access to the RDS instances.

EC2 instances that use the security group assigned to them in the private subnets will be able to communicate with the RDS instances because the security group rules are set to allow this specific traffic.

This approach ensures that only instances in the private subnets, which have the appropriate security group assigned to them, can access the RDS databases while isolating them from instances in the public subnets. It's a common practice for security and access control in AWS VPC architectures.

Question 77
A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website.
The company has noticed that some insert operations are taking 10 seconds or longer. The company has determined that the database storage performance is the problem.

Which solution addresses this performance issue?

A. Change the DB instance to a memory optimized instance class.

B. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

C. Change the DB instance to a burstable performance instance class.

D. Change the storage type to Provisioned IOPS SSD.**Correct answer**

Overall explanation
General Purpose (SSD) storage provides a balance of price and performance, but it might not be suitable for workloads with high write-intensive operations.

Provisioned IOPS SSD (io1) storage allows you to allocate a specific number of IOPS (Input/Output Operations Per Second) and provides consistent and predictable performance. This can significantly improve write performance, especially for workloads with frequent updates.

Changing the instance type or enabling Multi-AZ RDS read replicas won't directly address the storage performance issue related to high write-intensive operations.

Question 78
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 RDS.

B. Migrate the file share to Amazon Elastic File System (Amazon EFS).

C. Migrate the file share to AWS Storage Gateway.

D. Migrate the file share to Amazon FSx for Windows File Server.**Correct answer**

Overall explanation
The most resilient and durable replacement for the on-premises file share in this scenario would be Amazon FSx for Windows File Server.

Amazon FSx is a fully managed Windows file system service that is built on Windows Server and provides native support for the SMB protocol. It is designed to be highly available and durable, with built-in backup and restore capabilities.

It is also fully integrated with AWS security services, providing encryption at rest and in transit, and it can be configured to meet compliance standards.

Question 79

A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.

Which solution will meet these requirements?

A. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.

B. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.**Correct answer**

C. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).

D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

Overall explanation

Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.

Explanation:
To set up a secure API Gateway with a custom domain and an SSL certificate for third-party services, you should follow these steps:

Create a Regional API Gateway endpoint, as this allows you to associate it with a custom domain name.

Import the public certificate associated with your company's domain name into AWS Certificate Manager (ACM). Make sure the ACM certificate is in the same AWS Region as your API Gateway for easy association.

Attach the ACM certificate to the API Gateway endpoint.

Configure Route 53 to route traffic to the API Gateway endpoint, by setting up the appropriate DNS records.

This approach ensures that your API Gateway is associated with your custom domain name and secured using an SSL certificate, making it accessible via HTTPS for the third-party services.

Question 80
A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.
The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

A. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

B. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.**Correct answer**

C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.

D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Overall explanation
Kinesis Data Firehose is a fully managed service that makes it easy to ingest, transform, and load data streams into various AWS services, including Amazon S3.

Storing the data in Amazon S3 is highly durable, cost-effective, and scalable. You can configure S3 to transition data to Amazon S3 Glacier after 14 days, which aligns with your requirements for archiving data older than 14 days.

This solution minimizes operational overhead because it doesn't require you to manage additional infrastructure, such as EC2 instances, Elastic Load Balancers, or Elasticsearch clusters.

Data transition to S3 Glacier ensures cost savings for long-term data retention.

Question 81
A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud.
Which solution will meet these requirements?

A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.

B. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

C. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.

D. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.**Correct answer**

Overall explanation
AWS Network Firewall: AWS Network Firewall is a managed firewall service that allows you to create custom rules for filtering and inspecting network traffic. It's designed for precisely this type of traffic inspection and filtering use case.

Custom Rules: You can define custom rules in AWS Network Firewall to perform deep packet inspection, filtering, and other traffic management tasks to meet your specific requirements.

Question 82
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. io1 volume type

C. GP3 volume type **Correct answer**

D. io2 volume type

Overall explanation
GP3 volume type

Explanation:
Independent Performance: GP3 volumes provide independent performance of IOPS and throughput, allowing for high IOPS performance regardless of storage capacity.

Cost-Effective: GP3 volumes are cost-effective and allow for fine-tuning of performance based on specific requirements.

Provisioned IOPS: GP3 allows provisioning of IOPS based on application needs, ensuring high IOPS performance for the given workload.

Flexible Storage Capacity: GP3 volumes offer flexibility in storage capacity, aligning with the requirement to provision disk performance independent of storage capacity.

Ideal for Bursty Workloads: GP3 is suitable for bursty workloads, making it cost-effective while meeting the daily peak IOPS requirements.

Question 83
A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

A. S3 One Zone-Infrequent Access (S3 One Zone-IA)

B. S3 Standard-Infrequent Access (S3 Standard-IA)

C. S3 Intelligent-Tiering **Correct answer**

D. S3 Standard

Overall explanation

Resilience: S3 Intelligent-Tiering provides the same durability and availability as S3 Standard. It replicates objects across multiple Availability Zones, ensuring resiliency to the loss of an Availability Zone.

Cost-Efficiency: S3 Intelligent-Tiering automatically moves objects between the frequent and infrequent access tiers based on changing access patterns. This means you pay lower storage costs for infrequently accessed files, and it adjusts to your unpredictable access pattern without manual intervention. This cost-effective approach is ideal for files with varying access frequencies.

Question 84

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, 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.

B. 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.

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.**Correct answer**

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.

Overall explanation
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.

Explanation:
Compute Savings Plan: Purchasing a Compute Savings Plan provides cost savings for both EC2 instances and Lambda functions, optimizing expenses.

Optimizing Lambda Functions: Optimizing duration, memory usage, invocations, and data transfer helps in maximizing the efficiency of Lambda functions.

Private Subnet Access: Connecting Lambda functions to the private subnet ensures direct network access to EC2 instances, meeting the application's requirements.

Least Privilege: Placing Lambda functions in the private subnet adheres to the principle of least privilege, enhancing security.

Minimizing Latency: Connecting to resources within the same private subnet minimizes network latency between Lambda functions and EC2 instances.

Question 85
A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day.
The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.

What should a solutions architect do to meet these requirements?

A. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to the S3 File Gateway. Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.

B. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway. depending on each workload's location.

C. Deploy and configure Amazon FSx for Windows File Server on AWS. Deploy and configure an Amazon FSx File Gateway on premises. Move the on-premises file data to the FSx File Gateway. Configure the cloud workloads to use FSx for Windows File Server on AWS. Configure the on-premises workloads to use the FSx File Gateway.**Correct answer**

D. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.

Overall explanation
The Amazon FSx File Gateway extends Amazon FSx for Windows File Server to any site with an internet connection. It provides a scalable local cache, up to 64 TB, for low latency access to most recently used files.

By deploying an Amazon FSx File Gateway within your data center or remote and branch offices, your Windows clients are able to connect over the LAN.

As Amazon FSx File Gateway is a local cache of most recently accessed data backed by an Amazon FSx file system, it looks like a local file server to users and applications.

Question 86
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 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.**Correct answer**

B. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.

C. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.**Correct answer**

D. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block 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.

Overall explanation
To allow communication between the web servers and the database securely, it's best to create a security group for the DB instance and allow traffic from the security group of the web servers on port 3306.

Allowing inbound traffic on port 443 from 0.0.0.0/0 for the web servers in the public subnet ensures accessibility to the application over HTTPS from anywhere.

Question 87
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.

B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALUse the managed renewal feature to automatically rotate the certificate.

C. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.**Correct answer**

D. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.

Overall explanation
Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

With this approach, you import the third-party certificate into ACM, which allows you to centrally manage and apply it to the ALB. By configuring CloudWatch Events, you can receive notifications when the certificate is close to expiring, prompting you to manually initiate the rotation process.

Question 88
A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions.
The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.

B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.

C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.**Correct answer**

D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Overall explanation
Network Load Balancer (NLB): NLB is designed to handle TCP/UDP traffic and is a good fit for VoIP services that use UDP connections.

Target Group: Associate the NLB with a target group, which allows you to connect the NLB to the Auto Scaling group.

Amazon Route 53 Latency Record: Create an Amazon Route 53 latency-based record set. This record will route users to the Region with the lowest latency based on their geographical location. Amazon Route 53 can resolve DNS queries to the closest AWS Region, helping ensure the lowest latency routing.

Amazon CloudFront: Utilize Amazon CloudFront with the Amazon Route 53 latency record as an origin. Amazon CloudFront can provide a content delivery network (CDN) to cache and serve content closer to end-users, further reducing latency.

Question 89
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?

Use an Amazon RDS Multi-AZ DB cluster deployment Point the read workload to the reader endpoint.**Correct answer**

Use an Amazon RDS Multi-AZ DB duster deployment Create two read replicas and point the read workload to the read replicas.

Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.

Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.

Overall explanation
Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.

Explanation:
Multi-AZ DB Cluster Deployment: Amazon RDS Multi-AZ deployment provides high availability and automatic failover support, meeting the requirement for a highly available database.

Read Replicas: Utilizing read replicas offloads read operations from the primary instance, enhancing overall database performance.

Reader Endpoint: The reader endpoint automatically directs read traffic to the appropriate replica, distributing the workload and minimizing load on the primary instance.

Automatic Failover Support: In case of a failure, Multi-AZ deployment ensures automatic failover to a standby replica in less than 40 seconds.

Cost-Effective: The combination of Multi-AZ deployment and read replicas allows for efficient scaling and cost-effective utilization of database resources.

Question 90
A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.
The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without

losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

A. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.**Correct answer**

C. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS

D. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.

Overall explanation
Amazon S3 File Gateway: Amazon S3 File Gateway allows you to extend your storage capacity using Amazon S3 as the back end. It provides low-latency access to frequently accessed files and seamlessly integrates with your on-premises file server.

S3 Lifecycle Policy: S3 provides a robust lifecycle management feature that can automatically transition data to lower-cost storage classes such as S3 Glacier Deep Archive after a specified number of days (in this case, 7 days). This ensures that rarely accessed files are archived, saving storage costs while still being accessible.

Question 91
A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (Cloud Watch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.

B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.**Correct answer**

C. Create an Auto Scaling group so that EC2 instances can scale out. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Overall explanation
Amazon AppFlow simplifies the process of transferring data between SaaS sources and S3, reducing the operational overhead required for handling data ingestion.

Configuring S3 event notifications to send events to an SNS topic when uploads are complete ensures that the notification functionality remains intact without significant overhead.

This solution offloads the data transfer process to AppFlow, making it more efficient and reducing the workload on the EC2 instances.

Question 92
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 a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.**Correct answer**

B. 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.

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 in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.

Overall explanation
AWS WAF (Web Application Firewall) provides protection against common web exploits. Using a rate-based rule in a web ACL allows you to set thresholds for request rates, helping to mitigate HTTP flood attacks with minimal operational overhead.

Regional AWS WAF web ACL is a managed web application firewall that can be used to protect your API Gateway API from a variety of attacks, including HTTP flood attacks. Rate-based rule is a type of rule that can be used to limit the number of requests that can be made from a single IP address within a specified period of time.

API Gateway stage is a logical grouping of API resources that can be used to control access to your API.

Question 93
A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.
What should a solutions architect do to meet these requirements?

A. Move the catalog to Amazon ElastiCache for Redis.

B. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.

C. Deploy a larger EC2 instance with a larger instance store.

D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.**Correct answer**

Overall explanation
Amazon Elastic File System (Amazon EFS) is a scalable and highly available file storage service. It is designed to provide file storage that can be accessed from multiple EC2 instances in different Availability Zones, ensuring data durability and availability.

High Availability: Amazon EFS is a highly available and scalable file storage service. It's designed to provide a shared file system that can be accessed by multiple Amazon EC2 instances in different Availability Zones within an AWS Region. This means that even if one Availability Zone experiences issues, your data remains accessible from other instances in different zones, ensuring high availability.

Data Durability: Amazon EFS is designed for durability. Your data is automatically replicated across multiple Availability Zones, which makes it resilient to hardware failures or other issues that could affect a single instance. The data is stored redundantly, so there's a very low risk of data loss.

Ease of Use: With Amazon EFS, you can easily mount the shared file system on your EC2 instances. This allows your website to access the catalog data like it would from a regular file system. It simplifies data access and management.

Scalability: Amazon EFS can automatically grow and shrink with your data storage needs. You don't need to worry about provisioning the right amount of storage upfront, and it's cost-effective.

Question 94
A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions.
Which solution will meet these requirements with the LEAST operational overhead?

A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.**Correct answer**

B. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.

C. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter. Use multi-Region secret replication for the required Regions. Configure Systems Manager to rotate the secrets on a schedule.

D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys. Store the secrets in an Amazon DynamoDB global table. Use an AWS Lambda function to retrieve the secrets from DynamoDB. Use the RDS API to rotate the secrets.

Overall explanation
AWS Secrets Manager: AWS Secrets Manager is designed specifically for securely managing and rotating credentials. It offers a built-in capability to manage and automatically rotate secrets.

Multi-Region Secret Replication: AWS Secrets Manager allows you to replicate secrets to multiple AWS Regions, ensuring that the credentials are available in the required Regions.

Automatic Rotation: AWS Secrets Manager can be configured to rotate secrets automatically on a schedule, which reduces operational overhead and enhances security.

Question 95
A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit access at all levels of the stored data.

The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.

Which solution will meet these requirements?

A. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

C. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.**Correct answer**

D. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.

Overall explanation

- Data sync is used for migrate. Storage gw is used to connect on-prem to AWS.

- Data Events is to log for access, management events is for config or management

Question 96

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. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing.

B. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.

C. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.**Correct answer**

D. Set the Lambda function's runtime timeout value to 15 minutes.

Overall explanation
Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Explanation:
Introducing Amazon SQS as a buffer between the S3 event and the Lambda function can help decouple the processing and improve the architecture's resilience.

SQS can act as an event queue, and Lambda can be configured to process items from the SQS queue.

This allows for better management of the workload, handling peaks efficiently, and avoiding the loss of documents during heavy traffic.

Question 97
A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.
What should a solutions architect do to accomplish this goal?

A. Create an Amazon S3 bucket to store objects that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.

B. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

C. Use AWS Secrets Manager. Turn on automatic rotation.**Correct answer**

D. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.

Overall explanation
AWS Secrets Manager: AWS Secrets Manager is a service designed for secure and efficient management of credentials, secrets, and other sensitive information. It provides a central and secure repository for storing database credentials.

Automatic Rotation: AWS Secrets Manager allows you to enable automatic credential rotation. This feature helps enhance security by automatically rotating database credentials, reducing the risk associated with long-lived credentials. It also minimizes operational overhead because credential rotation is automated, reducing manual management tasks.

Question 98
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. 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.

C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.

D. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.**Correct answer**

Overall explanation
Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.

This option requires the least administrative overhead because:

- It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.

- The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.

- All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.

Question 99
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?

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).

Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.

Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.**Correct answer**

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.

Overall explanation
Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.

Explanation:
S3 Lifecycle Configuration: Automating the transition of objects based on access patterns is achieved through S3 Lifecycle policies.

S3 Intelligent-Tiering: It automatically moves objects between two access tiers (frequent and infrequent access) based on changing access patterns.

Least Operational Overhead: S3 Intelligent-Tiering requires no manual intervention for object movement, minimizing operational overhead.

Cost Optimization: Automatically moving objects to the most cost-effective storage class based on access patterns helps optimize costs.

Adaptive to Varying Access: S3 Intelligent-Tiering adapts to varying access patterns without the need for explicit management.

Question 100
A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.

Which solution meets these requirements MOST cost-effectively?

A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.

B. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

C. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.

D. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.**Correct answer**

Overall explanation
By using Amazon CloudFront in front of your S3 bucket, you can reduce latency for users accessing the website.

CloudFront has a global network of edge locations, which will cache and serve content from the edge locations closest to the users.

This helps to improve latency and reduces the load on the S3 bucket, making it a cost-effective solution for decreasing latency for a static website.

Question 101
The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

What are the effective IAM permissions of this policy for group members?

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

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

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

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

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

Explanation:

IAM Policy Statements: The policy includes specific statements allowing ec2:StopInstances and ec2:TerminateInstances actions with conditions.

Region-Specific Permissions: Permissions are specified for the us-east-1 Region, limiting the scope of the actions to a specific region.

Multi-Factor Authentication (MFA): Additional conditions require users to be logged in with MFA to perform certain actions, enhancing security.

Wildcard Permission: The policy permits any other EC2 action within the specified region, providing flexibility for other actions.

Granular Access Control: The policy enforces granular access control, allowing only specific actions under specific conditions within the defined region.

Question 102
A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

Which solution will meet these requirements with the LEAST operational overhead?

A. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.**Correct answer**

B. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.

D. Use the EC2 serial console to directly access the terminal interface of each instance for administration.

Overall explanation
AWS Systems Manager Session Manager allows you to securely access your EC2 instances without needing to use SSH keys or open inbound ports in your security groups.

By attaching IAM roles to your EC2 instances and using Session Manager, you can achieve secure and controlled remote access, and it aligns with AWS Well-Architected best practices.

This approach minimizes operational overhead and provides a more streamlined and secure remote administration process.

Question 103
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.**Correct answer**

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 IP addresses of the customers.

C. 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.

D. 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.

Overall explanation

It allows HTTPS access from any public IP address, meeting the requirement for global customer access.

HTTPS provides encryption for secure communication.

And for the database security group, only allowing inbound port 3306 from the web server security group properly restricts access to only the resources that need it.

Question 104

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 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. Process the data in Amazon ECS.

B. 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. Process the data in Amazon ECS.

C. 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.

D. 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 NLProcess the data in Amazon ECS.**Correct answer**

Overall explanation
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. Process the data in Amazon ECS.

Explanation:
AWS Global Accelerator combined with Network Load Balancers (NLBs) in multiple regions provides a scalable and resilient solution. Amazon ECS with Fargate launch type allows for serverless container management.

Question 105
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 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.**Correct answer**

B. 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.

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 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.

Overall explanation
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.

Explanation:
Elastic File System (Amazon EFS): EFS provides scalable and highly available file storage, suitable for a serverless SFTP service.

Encrypted Volume: The requirement for encryption is met by creating an encrypted EFS volume, ensuring data security.

AWS Transfer Family SFTP Service: AWS Transfer Family allows for the creation of a fully managed SFTP service with high configurability and security.

VPC Endpoint with Elastic IP Addresses: Using a VPC endpoint with elastic IP addresses ensures secure access to the SFTP service from trusted IP addresses over the internet.

Security Group: Attaching a security group to the endpoint allows fine-grained control over inbound traffic, limiting access to trusted IP addresses.

Maintaining Control over User Permissions: IAM roles and policies can be used to control user permissions and maintain control over user access to the SFTP service.