# COHORT 3

# AWS SOLUTIONS ARCHITECT ASSOCIATE PRACTICE QUESTIONS 2

## 105 QUESTIONS

**Question 1**

**A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.**

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

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.

B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.

C. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.Correct selection

D. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

E. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.Correct selection

**Overall explanation**

Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company. This ensures that only the company's external IP addresses can access the bastion host.

Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host. This restricts SSH access to the application instances to traffic originating from the bastion host, enhancing security.

**Question 2**
**A company that uses AWS is building an application to transfer data to a product manufacturer. The company has its own identity provider (IdP). The company wants the IdP to authenticate application users while the users use the application to transfer data. The company must use Applicability Statement 2 (AS2) protocol.**

**Which solution will meet these requirements?**

A. Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.**Correct answer**

B. Use Amazon AppFlow flows to transfer the data. Create an Amazon Elastic Container Service (Amazon ECS) task for IdP authentication.

C. Use AWS DataSync to transfer the data. Create an AWS Lambda function for IdP authentication.

D. Use AWS Storage Gateway to transfer the data. Create an Amazon Cognito identity pool for IdP authentication.

**Overall explanation**
Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.

- AWS Transfer Family supports the AS2 protocol, making it suitable for secure data transfer.
- AWS Lambda can be used to implement the necessary authentication logic with the company's identity provider.

**Question 3**
**A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in anotherAWS Region with minimal downtime.**

**What should a solutions architect do to meet these requirements with the LEAST amount of downtime?**

A. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

B. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

C. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed Configure DNS failover to point to the new disaster recovery Region's load balancer.

D. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.**Correct answer**

**Overall explanation**
Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

**Explanation:**

1. Global DynamoDB Table: Configuring the DynamoDB table as a global table allows for multi-region replication, ensuring data availability and low-latency access in the disaster recovery Region.
2. Auto Scaling and Load Balancer: Using an Auto Scaling group and load balancer in the disaster recovery Region ensures scalability and distribution of traffic to instances.
3. DNS Failover: Configuring DNS failover allows for seamless redirection of traffic to the disaster recovery Region's load balancer in case of a failover event.
4. Minimal Downtime: This solution provides minimal downtime during the failover process, ensuring continuous availability for users.
5. Cost-Effective: By utilizing Auto Scaling, load balancing, and global DynamoDB tables, this solution is cost-effective and aligns with the requirement for minimal operational overhead.

**Question 4**

**A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.**

**What should a solutions architect do to accomplish this?**

A. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

B. Use Amazon S3 with Transfer Acceleration to host the application

C. Use Amazon S3 with CacheControl headers to host the application.

D. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.**Correct answer**

**Overall explanation**

Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.

**Explanation:**

1. Amazon EC2 with Auto Scaling: Enables the application to scale based on demand, ensuring optimal performance during varying workloads.
2. Amazon CloudFront: A content delivery network (CDN) that accelerates content delivery by caching data at edge locations, reducing latency for users globally.
3. Minimize Latency: CloudFront caches and delivers content from the edge locations closest to end users, minimizing latency.
4. Cost-Effective: CloudFront helps optimize costs by reducing the load on EC2 instances and providing efficient content delivery.
5. Scalability: Using EC2 Auto Scaling ensures that the application can handle varying traffic loads while maintaining performance.

**Question 5**

**A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.**

**Which solution will meet these requirements?**

A. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan.**Correct answer**
B. Use Amazon S3 File Gateway to create the backup. Configure the appropriate S3 Lifecycle management.
C. Use AWS Backup to create a backup vault that has a vault lock in governance mode. Create the required backup plan.
D. Use Amazon Data Lifecycle Manager to create the required automated snapshot policy.

**Overall explanation**

Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan:

- AWS Backup provides centralized backup management for multiple services, including EC2 and S3.

- A backup vault with a vault lock in compliance mode ensures that backup data cannot be deleted or altered for the duration of the retention period.
- This approach aligns with the regulatory requirements of retaining backup files without alteration.

**Question 6**
**A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.**
**There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.**
**What should a solutions architect do to increase the application's performance?**

A. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.

B. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.

C. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.**Correct answer**

D. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.

**Overall explanation**
Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

By using AWS Certificate Manager (ACM) and an Application Load Balancer (ALB), you can offload the SSL/TLS encryption and decryption from the EC2 instances to the ALB. This helps improve the performance of your web application and reduces the load on the instances, making it a more scalable and efficient solution.

**Question 7**

**A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.**

**What should a solutions architect do to meet these requirements?**

A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.**Correct answer**

B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.

D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

**Overall explanation**

To meet the requirements of running stateless applications in containers that can tolerate disruptions while minimizing cost and operational overhead, you should use Spot Instances. Spot Instances provide a cost-effective way to run your workloads while allowing you to take advantage of available spare capacity in the AWS cloud.

**Question 8**

**A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.**

**The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.**

**What should a solutions architect do to meet these requirements?**

A. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected. the application will restart.

B. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.**Correct answer**

D. Enable HTTP health checks on the NLB, supplying the URL of the company's application.

**Overall explanation**

Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.

Here's why this option is a good choice:

1. Application Load Balancer (ALB): Unlike Network Load Balancer (NLB), Application Load Balancer (ALB) is designed to perform layer-7 (HTTP) health checks by default. It can check the actual content and response codes of your application to determine the health of instances. This is crucial for monitoring and managing application-level health.
2. HTTP Health Checks: By enabling HTTP health checks and supplying the URL of the company's application, ALB will regularly check the application's response. If it detects HTTP errors, it will mark the target instances as unhealthy, ensuring that traffic is not directed to them.
3. Auto Scaling Action: By configuring an Auto Scaling action to replace unhealthy instances, you ensure that when an instance is marked as unhealthy due to HTTP errors, it is automatically replaced with a new healthy instance. This automated recovery mechanism ensures improved availability without manual intervention.

**Question 9**

**A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high the workload does not process orders fast enough.**

**What should a solutions architect do to write the orders reliably to the database as quickly as possible?**

A. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.

B. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.

C. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.**Correct answer**

**Overall explanation**

Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database:

- Amazon SQS is a fully managed message queuing service that decouples components of a cloud application, making it highly scalable and reliable.
- By using SQS to buffer orders, the system can handle traffic bursts more effectively and ensures reliability.
- EC2 instances in an Auto Scaling group can scale based on demand, providing flexibility in handling varying workloads.

- An Application Load Balancer can distribute traffic among instances, ensuring efficient order processing.

This solution provides a scalable and reliable way to handle high traffic periods.

**Question 10**
**A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.**
**Which solution will satisfy these requirements?**

A. Configure Amazon EFS storage and set the Active Directory domain for authentication.

B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.

C. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.**Correct answer**

D. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.

**Overall explanation**
Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Amazon FSx for Windows File Server is a managed Windows file system that integrates with AWS Directory Service, allowing you to set up Active Directory authentication and access control. This solution is highly available and designed for Microsoft workloads like SharePoint that require Windows shared file storage. Amazon FSx provides features such as automatic backups, multi-AZ deployment, and high performance, making it a suitable choice for this use case.

**Question 11**
**A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.**
**Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files.**

**Which solution meets these requirements with the LEAST operational overhead?**

A. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

B. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.**Correct answer**

D. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.

**Overall explanation**

Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.

This solution is the most suitable for processing small files quickly and with minimal operational overhead. Here's why:

1. Amazon S3 event notifications are used to trigger the processing when a new file is uploaded, ensuring a quick response to user uploads.
2. An SQS queue acts as a buffer for incoming processing requests, allowing you to handle variable demand effectively.
3. AWS Lambda functions can be easily configured to process messages from the SQS queue, and they can be automatically scaled as needed.
4. Storing the resulting JSON files in Amazon DynamoDB is a suitable option, especially if you need to quickly access and analyze the processed data.

This approach is both scalable and cost-effective, as you only pay for the actual usage of AWS Lambda and other services when processing files. It requires minimal management and operational overhead.

**Question 12**

**A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement. new documents cannot be modified or deleted after they are stored.**

**What should a solutions architect do to meet this requirement?**

A. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.

B. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.

D. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.**Correct answer**

**Overall explanation**

Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.

Here's why this option is appropriate:

1. S3 Versioning: Enabling S3 Versioning ensures that every object version is preserved when changes are made. This means that when users upload a new version of a document, it's stored as a new version while retaining the old one. This prevents accidental or malicious modifications or deletions because all versions are kept.
2. S3 Object Lock: By enabling S3 Object Lock, you can set retention periods and legal holds on objects, ensuring that once an object is created and locked, it can't be deleted or modified until the lock period expires or is removed. This is especially important for regulatory compliance and data immutability.

Using these S3 features will help you meet the requirement effectively, keeping the documents safe from accidental or unauthorized changes or deletions.

**Question 13**

**A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.**

**What should a solutions architect recommend?**

A. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

B. Create a DynamoDB table in on-demand capacity mode.

C. Create a DynamoDB table with a global secondary index.

D. Create a DynamoDB table with provisioned capacity and auto scaling.**Correct answer**

**Overall explanation**

Create a DynamoDB table with provisioned capacity and auto scaling.

Provisioned capacity provides the company with predictable costs, which can be helpful when cost optimization is a concern. The addition of auto scaling ensures that the table can handle traffic spikes during unpredictable evenings efficiently without overprovisioning and incurring unnecessary costs during the morning when the table is not in use. Auto scaling automatically adjusts capacity based on traffic patterns, making it an ideal choice for workloads with unpredictable traffic spikes. This way, the company pays for the capacity it needs during high-traffic periods and can scale down during low-traffic periods.

**Question 14**

**A company stores data in PDF format in an Amazon S3 bucket. The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.**

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

A. Turn on the S3 Versioning feature for the S3 bucket. Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.

B. Turn on S3 Object Lock with governance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.

C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.**Correct answer**

D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

**Overall explanation**

Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.

**Explanation:**

1. S3 Object Lock with Compliance Retention Mode: Ensures that objects cannot be deleted or overwritten for a specified retention period, meeting legal retention requirements.
2. Least Operational Overhead: Once S3 Object Lock with compliance retention is configured, it requires minimal ongoing operational overhead.
3. Retention Period: Setting the retention period to 7 years aligns with the legal requirement for data retention.
4. Existing Data Compliance: Recopying existing objects is a one-time operation to bring them into compliance with the retention policy.
5. Data Immutability: S3 Object Lock ensures the immutability of objects during the retention period, providing data integrity and compliance.

**Question 15**

**An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.**

**What should the solutions architect recommend?**

A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.

B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.

C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.

D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.**Correct answer**

**Overall explanation**

Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Creating read replicas is the best approach to separate read traffic from write traffic and improve application performance. Read replicas allow read-intensive workloads to be offloaded from the primary database, reducing the load on the source database. In this case, configuring the read replicas with the same compute and storage resources as the source database ensures that they can handle the read traffic effectively and provide better performance.

**Question 16**

**A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours.**

**The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.**

**Which solution will meet this requirement with the LEAST operational overhead?**

A. Instruct the development team to manually export the entries in the database at the end of each day.

B. Create a read replica of the database. Configure the script to query only the read replica.**Correct answer**

C. Modify the DB instance to be a Multi-AZ deployment.

D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

**Overall explanation**
Create a read replica of the database. Configure the script to query only the read replica.

By creating a read replica of the database, you can offload the read queries from the primary database to the read replica. This reduces the impact of the script's read queries on the primary database's performance, allowing it to continue serving production traffic without disruption. You can configure your script to query the read replica, ensuring that it does not affect the primary database's performance.

Using read replicas is a common method to scale read-heavy workloads and improve database performance without changing the primary database's configuration. It is a relatively low-overhead solution in terms of operational effort.

**Question 17**
**A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.**
**The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.**
**A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.**

**Which solution meets these requirements?**

A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.**Correct answer**

C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

**D.** Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.

**Overall explanation**

Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

With Amazon Aurora, you can create a clone of the production database for the staging environment almost instantly without impacting the production database. This approach ensures minimal application latency during cloning and allows the development team to use the staging environment effectively. Additionally, Amazon Aurora offers better performance and scalability than traditional MySQL databases.

**Question 18**

**A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.**

**Which design should a solutions architect recommend?**

A. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.

C. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.

D. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.**Correct answer**

**Overall explanation**

Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.

This approach leverages RDS event notifications to trigger actions when the database on Amazon RDS is updated. When an automobile is sold, an RDS event notification can be sent to an Amazon SQS queue, and that queue can then fan out to multiple Amazon SNS topics. AWS Lambda functions can be used to process these SNS notifications and update the multiple target systems as needed. This design provides flexibility and decoupling of components, making it a suitable choice for the scenario described.

**Question 19**

**A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.**

**What should the solutions architect recommend?**

A. Implement EC2 On-Demand Instances.

B. Purchase EC2 Reserved Instances.

C. Implement the processing on AWS Lambda.

D. Implement EC2 Spot Instances.**Correct answer**

**Overall explanation**
Implement EC2 Spot Instances.

EC2 Spot Instances provide a cost-effective way to run workloads that are flexible regarding when they can run. Spot Instances allow you to take advantage of spare EC2 capacity, which can significantly reduce your compute costs. You can start and stop Spot Instances as needed, making them suitable for stateless and batch processing workloads like the one described. However, keep in mind that Spot Instances can be interrupted if the capacity they are using is needed for other workloads, so you should design your application to handle interruptions gracefully.

**Question 20**
**A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.**

**What should a solutions architect recommend?**

A. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.**Correct answer**

B. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.

C. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

D. Deploy Amazon Inspector and associate it with the ALB.

**Overall explanation**

Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.

**Explanation:**

1. AWS WAF for Web Application Firewall: AWS WAF provides protection against DDoS attacks and allows the creation of rules to filter and control incoming traffic.
2. Rate-Limiting Rule: Configuring a rate-limiting rule in AWS WAF helps control the request rate from illegitimate external systems, minimizing the impact on legitimate users.
3. Application Load Balancer (ALB): Associating AWS WAF with the ALB ensures that the filtering and rate limiting are applied at the entry point of the application.
4. Least Impact on Legitimate Users: Rate limiting allows the system to distinguish between legitimate and illegitimate traffic, minimizing the impact on legitimate users during a potential DDoS attack.
5. Scalability: AWS WAF scales with the application, providing effective protection without significant operational overhead.

**Question 21**

**A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.**

**How can the solutions architect meet this requirement?**

A. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.

B. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.

C. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.**Correct answer**

D. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.

**Overall explanation**

Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Using an S3 VPC gateway endpoint, the data transfer occurs over the AWS network without incurring data transfer fees, as it stays within the AWS network infrastructure of the same Region. This is a more efficient and cost-effective approach compared to routing through public subnets, NAT gateways, or internet gateways.

**Question 22**

**A company needs to migrate a MySQL database from its on-premises data center to AWS within 2 weeks. The database is 20 TB in size. The company wants to complete the migration with minimal downtime.**

**Which solution will migrate the database MOST cost-effectively?**

A. Order an AWS Snowball Edge Compute Optimized with GPU device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowball device to AWS to finish the migration and continue the ongoing replication

B. Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.**Correct answer**

C. Order a 1 GB dedicated AWS Direct Connect connection to establish a connection with the data center. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes.

**D.** Order an AWS Snowmobile vehicle. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowmobile vehicle back to AWS to finish the migration and continue the ongoing replication.

**Overall explanation**

Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.

**Explanation:**

1. AWS Snowball Edge: Snowball Edge provides a secure and efficient method for transferring large amounts of data, including the initial migration of a 20 TB database.
2. AWS DMS and SCT: AWS Database Migration Service (DMS) and Schema Conversion Tool (SCT) facilitate the migration process, including ongoing replication of changes.
3. Cost-Effective and Fast Migration: Snowball Edge is a cost-effective and fast solution for transferring large datasets, meeting the tight migration timeframe.
4. Minimize Downtime: Ongoing replication ensures minimal downtime during the migration process, allowing the company to continue operations seamlessly.
5. Operational Efficiency: This solution minimizes operational overhead by leveraging Snowball Edge for the initial migration and ongoing replication.

**Question 23**

**A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet.**

**Which solution will meet these requirements?**

A. Configure an S3 gateway endpoint.**Correct answer**

B. Create an S3 bucket in the same AWS Region as the EC2 instances.

C. Create an S3 bucket in a private subnet.

D. Configure a NAT gateway in the same subnet as the EC2 instances.

**Overall explanation**
Configure an S3 gateway endpoint.

An S3 gateway endpoint allows the EC2 instances in your VPC to access Amazon S3 securely without needing to route traffic over the internet. It keeps the traffic within your VPC network, providing both security and compliance with your company's regulations.

Options B and C are not sufficient by themselves to ensure that traffic does not travel across the internet, and Option D (NAT gateway) is typically used for enabling outbound internet access from private subnets, not for accessing Amazon S3.

**Question 24**
**A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate.**

**What should a solutions architect recommend to meet this requirement?**

A. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

B. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.

C. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).**Correct answer**

**Overall explanation**

Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert via Amazon Simple Notification Service (Amazon SNS).

Here's how it works:

1. Set up an Amazon EventBridge rule to trigger based on a schedule. Configure this rule to run daily and look for certificates that will expire within the next 30 days.
2. When the rule detects certificates that meet the criteria, it triggers an AWS Lambda function.
3. The Lambda function can send a custom alert via Amazon SNS to notify the security team about the certificates that are about to expire.

This solution automates the certificate expiration notifications and ensures timely alerts to the security team.

**Question 25**

**A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.**

**Which combination of steps should a solutions architect take to automate this task? (Choose two.)**

A. Manually use an operating system copy command to push the data to the EC2 instance.

B. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.

C. Install an AWS DataSync agent in the on-premises data center.**Correct selection**

D. Launch the EC2 instance into the same Availability Zone as the EFS file system.**Correct selection**

E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

**Overall explanation**

Launch the EC2 instance into the same Availability Zone as the EFS file system.

Install an AWS DataSync agent in the on-premises data center.

To migrate the data from the on-premises SFTP server to an EC2 instance hosted on Amazon EFS, you should take the following steps:

1. Launch an EC2 instance into the same Availability Zone as the Amazon EFS file system to minimize data transfer costs and latency.
2. Install an AWS DataSync agent in your on-premises data center to facilitate the data transfer. AWS DataSync is a managed data transfer service that can help automate the data migration process. You can configure it to efficiently transfer data from your on-premises location to Amazon EFS on the EC2 instance.

**Question 26**

**A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost**

**usage tags.**

**Which solution will meet these requirements?**

A. Create a custom trail in AWS CloudTrail to prevent tag modification.

B. Create custom Amazon CloudWatch logs to prevent tag modification.

C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.Correct answer

D. Create a custom AWS Config rule to prevent tag modification except by authorized principals.

**Overall explanation**

Create a service control policy (SCP) to prevent tag modification except by authorized principals.

**Explanation:**

1. Service Control Policies (SCPs): SCPs in AWS Organizations allow fine-grained control over permissions, including the ability to prevent tag modifications.
2. Organization-Wide Policy: SCPs apply at the organization level, ensuring consistent enforcement of tag modification restrictions across all accounts.
3. Preventing Unauthorized Changes: SCPs can explicitly deny modifications to specific tags, limiting tag changes to authorized principals only.
4. Least Operational Overhead: SCPs provide a centralized and low-operational-overhead solution for controlling and restricting actions across multiple accounts.
5. Effective Tag Governance: SCPs enhance tag governance by preventing unauthorized changes, ensuring tag consistency, and adhering to organizational policies.

**Question 27**

**A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application**

**across multiple AWS Regions to provide Regional failover capabilities.**

**What should a solutions architect do to route traffic to multiple Regions?**

A. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.

B. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.**Correct answer**

C. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

D. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.

**Overall explanation**

To route traffic to multiple AWS Regions and provide regional failover capabilities for a stateless web application running on AWS Lambda functions invoked by Amazon API Gateway, you can use Amazon Route 53 with an active-active failover configuration.

By creating Amazon Route 53 health checks for each Region and configuring an active-active failover configuration, Route 53 can monitor the health of the endpoints in each Region and route traffic to healthy endpoints. In the event of a failure in one Region, Route 53 automatically routes traffic to the healthy endpoints in other Regions.

This setup ensures high availability and failover capabilities for your web application across multiple AWS Regions.

**Question 28**

**A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested determines the access pattern on the S3 objects.**

**The company cannot predict or control the access pattern. The company wants to**

**reduce its S3 costs.**

**Which solution will meet these requirements?**

A. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)

B. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering.**Correct answer**

C. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA).

D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering.

**Overall explanation**

Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering:

- S3 Intelligent-Tiering: This storage class automatically moves objects between two access tiers – frequent and infrequent access – when access patterns change. It is designed to optimize costs for varying access patterns without any performance impact.

By using S3 Intelligent-Tiering, the company can ensure that objects are moved to the most cost-effective storage class based on their access patterns, reducing costs.

**Question 29**

**A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.**

**What should a solutions architect do to redesign the application MOST cost-effectively?**

A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.

B. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.**Correct answer**

D. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.

**Overall explanation**

Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.

**Explanation:**

1. Amazon CloudFront: It is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency.
2. Static Web Content: CloudFront can cache and serve static web content (like images, stylesheets, and scripts) from an Amazon S3 bucket, reducing the load on EC2 instances.
3. Cost Optimization: CloudFront helps optimize costs by caching and delivering content from edge locations, reducing the need for additional On-Demand Instances.
4. Global Distribution: CloudFront ensures low-latency access for users globally by distributing content through a network of edge locations.
5. Integration with S3: Hosting static content in an S3 bucket allows for easy management, versioning, and scalability.

**Question 30**

**A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.**

**Which solution resolves this issue with the LEAST operational overhead?**

A. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC Update the routes and create new resources in the subnets of the second VPC.

B. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPUpdate the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.

C. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.

D. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.**Correct answer**

**Overall explanation**

You assign a single CIDR IP address range as the primary CIDR block when you create a VPC and can add up to four secondary CIDR blocks after creation of the VPC.

**Question 31**

**A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.**

**Which solution will meet these requirements?**

A. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB.**Correct answer**

B. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.

C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin.

D. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.

**Overall explanation**

Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listens on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB:

- AWS Global Accelerator enhances the availability and performance of applications by using static IP addresses (Anycast).
- Network Load Balancer (NLB) is suitable for TCP and UDP traffic, making it ideal for gaming applications.
- NLB provides low-latency and high-throughput load balancing.

This solution ensures the lowest possible latency for global users while efficiently handling TCP and UDP traffic.

**Question 32**

**A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible. The data center does not have any available network bandwidth for additional**

**workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.**

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

A. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue.**Correct answer**

B. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.

C. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device.

D. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue.

**Overall explanation**

Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job using AWS Glue.

AWS Snowball Edge Storage Optimized is a suitable choice for transferring large amounts of data in a secure, efficient, and scalable manner. It allows you to move the 50 TB of data from your on-premises environment to AWS without adding extra network load to your existing infrastructure.

After transferring the data to the Snowball Edge, you can use AWS Glue for the data transformation job, which can be configured to run in the AWS Cloud. This approach minimizes operational overhead and ensures a seamless migration with the least impact on your existing systems.

**Question 33**

**A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an**

**Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.**

**Which combination of configuration options will meet these requirements? (Choose two.)**

A. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

B. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.

C. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.**Correct selection**

D. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.

E. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.**Correct selection**

**Overall explanation**

Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

- This option deploys EC2 instances in private subnets, ensuring that they are not directly exposed to the public internet, which is a good security practice.
- It also deploys the RDS DB instance in private subnets, which is another good practice for securing the database.

- However, the option does not address the requirement for the EC2 instances to have internet access for payment processing. Without a means to access the internet, the EC2 instances won't be able to communicate with third-party web services for payment processing.

Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

- This option places the EC2 instances in private subnets, ensuring they are not exposed to the public internet, which is a good security practice.
- It also deploys an Application Load Balancer (ALB) in private subnets, which is an effective way to distribute incoming traffic to the EC2 instances.
- To provide internet access to the EC2 instances for payment processing, it uses Network Address Translation (NAT) gateways, which are placed in public subnets. This allows the EC2 instances in private subnets to access the internet via the NAT gateways.

**Question 34**
**A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.**

**Which storage solution meets these requirements MOST cost-effectively?**

A. Amazon OpenSearch Service (Amazon Elasticsearch Service)

B. Amazon Elastic Block Store (Amazon EBS)

C. Amazon S3 **Correct answer**

D. Amazon Elastic File System (Amazon EFS)

**Overall explanation**

For a web application that needs to store and serve text documents totaling about 900 TB in size, while scaling to meet high demand, Amazon S3 (Simple Storage Service) would be the most cost-effective and scalable solution. Amazon S3 is designed for scalable and durable object storage, and it can handle large volumes of data. You can also configure it for high availability and low-latency access.

Amazon S3 is suitable for storing static content like text documents, and it can serve them to your web application efficiently, especially during periods of high demand. Additionally, you can easily configure features like multi-region replication, lifecycle policies, and access control to meet various requirements while optimizing costs.

**Question 35**

**A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.**

**Which solution offers the MOST reliable data transfer?**

A. AWS DataSync over AWS Direct Connect **Correct answer**

B. AWS Database Migration Service (AWS DMS) over public internet

C. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

D. AWS DataSync over public internet

**Overall explanation**

AWS DataSync over AWS Direct Connect offers the following advantages:

1. Low Latency: AWS Direct Connect provides a dedicated and private network connection from your on-premises data center to AWS. This ensures low latency, which is crucial for real-time analytics.
2. Reliable and Predictable Connectivity: AWS Direct Connect offers dedicated and consistent network connectivity, reducing the potential issues often associated with public internet connections.
3. Secure Transfer: DataSync over AWS Direct Connect provides a highly secure and controlled transfer of data. It encrypts data in transit and helps protect sensitive data.
4. Scalability: AWS DataSync can handle large data transfers efficiently, ensuring that your daily 10 TB of data is transferred reliably.

**Question 36**

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

**Which solution meets these requirements and is the MOST operationally efficient?**

A. Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation

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

C. Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation.**Correct answer**

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

**Overall explanation**

Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation.

Using Server-side encryption with AWS Key Management Service (SSE-KMS) with automatic rotation is the most operationally efficient solution as it provides automated key rotation and logs key usage, meeting the compliance requirements while minimizing the operational overhead of manual key rotation.

**Question 37**
**A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL in the database layer. Several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.**

**What should a solutions architect do to meet these requirements?**

A. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.**Correct answer**

B. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.

C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.

D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

**Overall explanation**
Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.

**Explanation:**

1. Real-time Scoreboard with Redis: Amazon ElastiCache for Redis is an in-memory data store that allows for real-time computation and caching, making it suitable for dynamic scoreboards.
2. Scalability: ElastiCache for Redis provides scalability, ensuring it can handle concurrent requests and computation for the top-10 scoreboard.
3. Near-Real Time: Redis supports low-latency operations, allowing the web application to display near-real-time scores for players.
4. Persistence: Redis can be configured for data persistence, allowing the preservation of scores even if the application is stopped or restored.

5. Ease of Integration: Redis can be easily integrated into the existing three-tier architecture, minimizing changes to the application.

**Question 38**

**A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.**

**The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.**

**Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?**

A. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

B. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

C. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

D. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.**Correct answer**

**Overall explanation**

Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.

**Here's why:**

1. Production EC2 instances run continuously, making them a good candidate for Reserved Instances (RIs). RIs offer cost savings compared to On-Demand instances for workloads that run 24/7. Ensure you choose the appropriate instance type and Availability Zone for your RIs to match your production workloads.
2. Development and test EC2 instances do not run continuously. Instead of Spot Instances, which can be terminated when capacity is reclaimed, On-Demand instances are a better choice if you want to ensure these instances are available whenever you need them. This simplifies the automation to stop and start these instances based on usage patterns.

By combining RIs for the production environment and On-Demand instances for the development and test environments, you can effectively reduce costs while maintaining the necessary flexibility and availability for your different use cases.

**Question 39**

**A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.**

**What should a solutions architect do to reduce the operational burden?**

A. **Use multi-factor authentication (MFA) to protect the encryption keys.**

B. **Use AWS Key Management Service (AWS KMS) to protect the encryption keys.Correct answer**

C. **Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.**

D. **Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.**

**Overall explanation**

Use AWS Key Management Service (AWS KMS) to protect the encryption keys.

AWS KMS is a managed service that makes it easy to create and control encryption keys for your applications. It helps you simplify key management tasks, including the creation, rotation, and protection of encryption keys. By using AWS KMS, you offload many of the operational aspects of key management to AWS, which can reduce the operational burden on your organization. Developers can use AWS KMS to encrypt and decrypt data without having to worry about key management tasks.

**Question 40**
**An application runs on Amazon EC2 instances across multiple Availability Zonas. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.**
**What should a solutions architect do to maintain the desired performance across all instances in the group?**

A. Use a simple scaling policy to dynamically scale the Auto Scaling group.

B. Use an AWS Lambda function to update the desired Auto Scaling group capacity.

C. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

D. Use a target tracking policy to dynamically scale the Auto Scaling group.**Correct answer**

**Overall explanation**
To maintain the desired performance across all instances in the Auto Scaling group, you should use a target tracking policy to dynamically scale the Auto Scaling group.

A target tracking policy allows you to set a specific metric (in this case, CPU utilization) as the target value. The Auto Scaling group will then automatically adjust the number of instances based on the desired metric value (e.g., maintaining CPU utilization around 40%).

**Question 41**
**A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.**

**Which solution will meet these requirements?**

A. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.

B. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.**Correct answer**

C. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.

D. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.

**Overall explanation**
Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS:

- REST API with Private VPC Link: This allows secure access to the backend services in private VPC subnets through a VPC link.

This solution aligns with the requirement of using REST APIs and accessing backend services in private VPC subnets.

**Question 42**
**A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.**

**What should a solutions architect recommend to resolve this issue?**

A. Create a NAT gateway and make it the destination of the subnet's route table

B. Create an egress-only internet gateway and make it the destination of the subnet's route table. **Correct answer**

C. Create an internet gateway and make it the destination of the subnet's route table

D. Create a virtual private gateway and make it the destination of the subnet's route table

**Overall explanation**
Create an egress-only internet gateway and make it the destination of the subnet's route table:

- Egress-only Internet Gateway: This is used for IPv6 traffic to allow outbound communication initiated by instances in a VPC while blocking inbound traffic.
- Security Policy Compliance: This solution aligns with the security policy that prohibits external services from initiating connections to EC2 instances.

This approach ensures that the EC2 instances can initiate outbound communications but are not reachable from the internet, meeting the security policy requirements.

**Question 43**
**A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.**

**What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?**

A. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

B. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.

C. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.

D. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance.**Correct answer**

**Overall explanation**

Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore an encrypted snapshot to an existing DB instance.

**Here's an explanation:**

1. By copying the snapshots and enabling encryption using AWS KMS, you ensure that both the existing snapshots and any future snapshots are encrypted.
2. Restoring an encrypted snapshot to an existing DB instance ensures that your database is always encrypted without the need to replace the existing DB instance.

This approach is the most appropriate to ensure encryption for both current and future snapshots while minimizing operational overhead. It leverages AWS KMS for encryption and provides data protection.

**Question 44**

**A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.**
**The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.**

**Which combination of actions should the solutions architect take to meet these requirements? (Choose two.)**

A. Configure the web server to upload the original images to Amazon S3.**Correct selection**

B. Configure the application to upload images to S3 Glacier.

C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL

D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.**Correct selection**

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

**Overall explanation**
Configure the web server to upload the original images to Amazon S3.

Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.

Uploading the original images directly from the web server to Amazon S3 eliminates the need to process the images on the web server, reducing coupling and improving website performance. Then, using S3 Event Notifications to trigger an AWS Lambda function to resize the images is an efficient way to handle the image processing without affecting user experience during the upload process. This offloads the resizing process to an asynchronous operation, further improving performance.

**Question 45**
**A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.**

A. Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan.

B. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.

C. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.

D. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.**Correct answer**

**Overall explanation**
Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account:

- Discount Sharing: AWS allows you to share Savings Plans and Reserved Instances discounts across the accounts within an organization in AWS Organizations.
- Billing Preferences: This can be configured at the organization level to share the discount benefits with member accounts.

By enabling discount sharing at the organization level, the company ensures that the member account receives the benefits of the Compute Savings Plan commitment, even if the workload changes within the account.

**Question 46**

**A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.**

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

A. **Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.**

B. **Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.**

C. **Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3. Correct answer**

D. **Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.**

**Overall explanation**

Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

**Here's why this is the most suitable option:**

1. Amazon Kinesis Data Streams and Amazon Kinesis Data Firehose are services specifically designed for real-time data ingestion, transformation, and delivery. They provide high scalability, reliability, and easy setup for streaming data.
2. Amazon API Gateway is used for managing APIs and receiving data from external sources.
3. AWS Lambda functions can be used for data transformation in real-time.
4. Amazon S3 is a highly scalable and durable storage solution for persisting the data.

**Question 47**

**A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.**

**What should a solutions architect do to secure the audit documents?**

A. **Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.**

B. **Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.**

C. **Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.**

D. **Enable the versioning and MFA Delete features on the S3 bucket.Correct answer**

**Overall explanation**

Enable the versioning and MFA Delete features on the S3 bucket.

By enabling versioning on the S3 bucket, it retains all versions of objects stored in the bucket. If an object is deleted, it is not actually removed; instead, it is marked as a "delete marker." This helps protect against accidental deletions because you can restore previous versions of objects. To delete a versioned object permanently, you need to use

Multi-Factor Authentication (MFA) Delete, which requires additional MFA authentication, making accidental deletions much less likely.

This approach provides a secure way to protect against accidental deletions without requiring IAM user accounts to have overly restrictive permissions. It also ensures that you can recover any deleted object versions if needed.

**Question 48**

**A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.**

**Which solution meets these requirements and is the MOST operationally efficient?**

A. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.

B. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

C. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.**Correct answer**

D. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.

**Overall explanation**

Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.

**Explanation:**

1. Amazon API Gateway: Amazon API Gateway allows you to create, publish, and manage RESTful APIs. It acts as an entry point for your application, providing API routing, request/response transformation, security, and other features. By directing transactions through API Gateway, you can efficiently manage and expose RESTful services.
2. AWS Lambda: AWS Lambda is a serverless compute service that can be used to run code in response to HTTP requests (among other triggers). You can create Lambda functions to serve as the application layer for your RESTful services. This serverless approach offers auto-scaling and abstracts the underlying infrastructure, making it operationally efficient.
3. Amazon SQS: Amazon SQS is a reliable and scalable message queue service that can be used as a communication layer between application services. It helps decouple the different tiers of your application, which can prevent transaction drops during load spikes or when one tier becomes overloaded.

**Question 49**

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

**Which storage solution is MOST cost-effective?**

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

B. **Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.**

C. **Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.**

D. **Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.Correct answer**

**Overall explanation**

Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.

**Here's the explanation:**

- S3 One Zone-Infrequent Access (S3 One Zone-IA) is a cost-effective storage class that provides infrequent access durability and availability in a single Availability Zone, which makes it a cost-effective choice for data that doesn't require the added resilience of multi-Availability Zone storage.
- The company's policy requires retaining the files for 4 years, and the most cost-effective approach is to transition them to a lower-cost storage class (S3 One Zone-IA) after the initial 30 days of frequent access.
- Deleting the files 4 years after creation aligns with the company's policy for data retention.

This approach minimizes costs while ensuring the data is accessible for the required 4-year retention period. Transitioning to S3 One Zone-IA after the initial 30 days allows for cost savings while retaining immediate accessibility.

**Question 50**

**A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources inventory. The solutions architect needs to build and map the relationship details of the various workloads across all accounts.**

**Which solution will meet these requirements in the MOST operationally efficient way?**

A. **Use AWS Step Functions to collect workload details. Build architecture diagrams of the workloads manually.**

B. **Use AWS Systems Manager Inventory to generate a map view from the detailed view report.**

C. **Use AWS X-Ray to view the workload details. Build architecture diagrams with relationships.**

D. **Use Workload Discovery on AWS to generate architecture diagrams of the workloads.** Correct answer

**Overall explanation**

Use Workload Discovery on AWS to generate architecture diagrams of the workloads.

- Workload Discovery on AWS helps discover and map relationships between resources.
- This is an efficient way to understand the inventory and relationships of various workloads across accounts.

**Question 51**

**A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function.**

**Which solution meets these requirements?**

A. **Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.** Correct answer

B. **Add an execution role to the function with lambda:InvokeFunction as the action and Service: lambda.amazonaws.com as the principal.**

C. **Add a resource-based policy to the function with lambda:* as the action and Service: events.amazonaws.com as the principal.**

D. **Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.**

**Overall explanation**
Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

To configure permissions for an AWS Lambda function invoked by an Amazon EventBridge (Amazon CloudWatch Events) rule, you should use a resource-based policy. This policy specifies the allowed actions (e.g., lambda:InvokeFunction) and the service principal (Service: events.amazonaws.com) that is invoking the function, which follows the principle of least privilege.

**Question 52**
**A company runs its application on an Oracle database. The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance. The application uses third-party database features that require privileged access.**

**Which solution will help the company migrate the database to AWS MOST cost-effectively?**

A. Migrate the database to Amazon RDS for Oracle. Replace third-party features with cloud services.

B. Migrate the database to an Amazon EC2 Amazon Machine Image (AMI) for Oracle. Customize the database settings to support third-party features.Correct answer

C. Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.

D. Migrate the database to Amazon RDS for PostgreSQL by rewriting the application code to remove dependency on Oracle APEX.

**Overall explanation**

**Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.**

**Question 53Skipped**

**A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS.**

**Which activities will be managed by the company's operational team? (Choose three.)**

A. Installation of patches for all minor and major database versions for Amazon RDS

B. Management of the Amazon RDS infrastructure layer, operating system, and platforms

C. Encryption of the data that moves in transit through Direct Connect

D. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window **Correct selection**

E. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection **Correct selection**

F. Ensure the physical security of the Amazon RDS infrastructure in the data center **Correct selection**

**Overall explanation**

Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window:

- Creating an Amazon RDS DB instance involves the operational task of provisioning the database.
- Configuring the scheduled maintenance window is part of managing the database maintenance tasks.

Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection:

- Amazon ECS, being a container service, requires additional configurations for monitoring, patch management, log management, and security components.
- These configurations are typically managed by the operational team.

Ensure the physical security of the Amazon RDS infrastructure in the data center:

- The physical security of the infrastructure in the data center, including Amazon RDS, is a responsibility of the operational team.

**Question 54**

**A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.**

**What should a solutions architect do to ensure messages are being processed once only?**

A. Use the ChangeMessageVisibility API call to increase the visibility timeout.**Correct answer**

B. Use the AddPermission API call to add appropriate permissions.

C. Use the CreateQueue API call to create a new queue.

D. Use the ReceiveMessage API call to set an appropriate wait time.

**Overall explanation**
Use the ChangeMessageVisibility API call to increase the visibility timeout.

**Here's the explanation:**

- The visibility timeout of an SQS message determines how long the message is invisible in the queue once it's received by a consumer. During this time, the message is effectively "locked" and cannot be processed by other consumers.
- By increasing the visibility timeout, you can make sure that the message stays invisible for a longer period while it is being processed by your application. This can help prevent multiple consumers from processing the same message concurrently and causing duplicate records in the RDS table.

Additionally, you should make sure that your application processes the message correctly and acknowledges the message only after it has been successfully processed. Increasing the visibility timeout provides a safety net to handle cases where processing takes longer than expected or to avoid concurrent processing of the same message.

The other options (A, B, and C) are not directly related to addressing the issue of occasional duplicate records in the RDS table caused by multiple processing of the same message.

**Question 55**
**A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.**

**Which combination of actions should the solutions architect take to accomplish this? (Choose two.)**

A. **Set up Amazon ElastiCache between the web application and the PostgreSQL database.**

B. **Migrate the PostgreSQL database to Amazon Aurora. Correct selection**

C. **Migrate the web application to be hosted on Amazon EC2 instances.**

D. **Set up an Amazon CloudFront distribution for the web application content.**

E. **Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).**

**Overall explanation**

Migrate the PostgreSQL database to Amazon Aurora: Amazon Aurora is a managed relational database service that can significantly reduce the operational burden of managing databases.

Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS): AWS Fargate is a serverless compute engine for containers, which eliminates the need to manage the underlying infrastructure. This can reduce operational overhead and simplify container management.

These two actions will help in improving scalability, manageability, and reduce the operational burden on the company's application infrastructure.

**Question 56**

**A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.**

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

A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the certificates as needed. Control access to the data by using fine-grained IAM access.

B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.

C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.**Correct answer**

D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.

**Overall explanation**

Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

By using AWS KMS for encryption and storing the encrypted data on Amazon EBS volumes, this solution provides a highly secure way to manage certificates and encrypt data. It's also straightforward and has relatively low operational overhead.

**Question 57**

**A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.**

**What should the solutions architect do to enable Internet access for the private subnets?**

A. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.

B. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only Internet gateway.

C. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ. **Correct answer**

**D.** Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.

**Overall explanation**

Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

To enable Internet access for the private subnets while ensuring high availability, it's common to use Network Address Translation (NAT) gateways in a Multi-AZ configuration. Each private subnet should have its own NAT gateway in the respective Availability Zone, and you associate each private subnet's route table with its corresponding NAT gateway. This design allows private instances to access the Internet for tasks like downloading software updates while preserving network security.

**Question 58**

**An ecommerce company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards.**

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

A. Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models. Use Amazon OpenSearch Service to visualize the data.

B. Use Amazon QuickSight to build and train models by using calculated fields. Use Amazon QuickSight to visualize the data.

C. Use AWS Glue to create an ML transform to build and train models. Use Amazon OpenSearch Service to visualize the data.

D. Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data. **Correct answer**

**Overall explanation**

Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.

**Explanation:**

1. Amazon SageMaker for ML Models: Amazon SageMaker is a fully managed service that makes it easy to build, train, and deploy machine learning models, reducing operational overhead.
2. QuickSight for Visualization: Amazon QuickSight is a business intelligence (BI) service that integrates seamlessly with SageMaker, allowing for easy visualization of ML model results.
3. Least Operational Overhead: SageMaker abstracts away the complexities of ML model management, reducing operational overhead for building and training models.
4. Integration with Reporting Platform: QuickSight can directly integrate with ML models built using SageMaker, providing a seamless flow of augmented data into business intelligence dashboards.
5. End-to-End Solution: SageMaker and QuickSight together offer an end-to-end solution for building, training, visualizing, and integrating ML models with reporting platforms.

**Question 59**

**A solutions architect is designing a RESTAPI in Amazon API Gateway for a cash payback service. The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.**

**Which additional combination ofAWS services will meet these requirements with the LEAST administrative effort? (Choose two.)**

A. Amazon EC2

B. Amazon Elastic Kubernetes Services (Amazon EKS)

C. AWS Lambda **Correct selection**

D. Amazon DynamoDB

E. Amazon RDS **Correct selection**

**Overall explanation**
**AWS Lambda:**

- AWS Lambda is a serverless compute service that is well-suited for small, periodic tasks.
- It can handle the periodic job efficiently without incurring costs when the job is not running.

**Amazon RDS:**

- Amazon RDS is a managed relational database service and can provide the required relational format for data.

**Question 60**
**A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs ta share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots.**

**What is the MOST secure way for the solutions architect to share the AMI with the**

**MSP Partner's AWS account?**

A. Make the encrypted AMI and snapshots publicly available. Modify the key policy to allow the MSP Partner's AWS account to use the key.

B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key. **Correct answer**

C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to trust a new KMS key that is owned by the MSP Partner for encryption.

D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account, Encrypt the S3 bucket with a new KMS key that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

**Overall explanation**

Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key.

This option ensures that the AMI and its snapshots remain secure. You modify the launchPermission property of the AMI to share it with the MSP Partner's AWS account, which allows the MSP Partner to access the AMI but not other AWS accounts. Additionally, you modify the key policy to allow the MSP Partner's AWS account to use the AWS KMS key used to encrypt the EBS volume snapshots. This ensures that the MSP Partner can use the key to access the encrypted data associated with the AMI while keeping the data secure and restricted to the authorized accounts.

**Question 61**

**A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The**

**company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.**

**Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)**

A. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled. **Correct selection**

B. Create and deploy an AWS Lambda function to manage and serve the website content.

C. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.

D. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

E. Configure Amazon CloudFront in front of the website to use HTTPS functionality. **Correct selection**

**Overall explanation**

Configure Amazon CloudFront in front of the website to use HTTPS functionality: Amazon CloudFront is a content delivery network (CDN) service that can distribute content globally and improve website performance. You can use CloudFront to provide enhanced security and scalability by distributing your website content to edge locations. Additionally, CloudFront supports HTTPS, which helps secure the data in transit between users and your website. This is a good option for providing both scalability and security.

Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled: Hosting a static website in an Amazon S3 bucket is a cost-effective and low operational overhead solution. It provides scalability, security, and simplified management, making it suitable for a website that is updated a few times a year and doesn't require dynamic content. Enabling static website hosting on an S3 bucket allows you to serve your website content directly from S3 while benefiting from Amazon S3's durability and scalability.

**Question 62**
**A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.**

**What should a solutions architect do to mitigate any single point of failure in this architecture?**

A. Add a second virtual private gateway and attach it to the Management VPC.

B. Add a second VPC peering connection between the Management VPC and the Production VPC.

C. Add a second set of VPNs to the Management VPC from a second customer gateway device. **Correct answer**

D. Add a set of VPNs between the Management and Production VPCs.

**Overall explanation**
Redundant VPN connections: Instead of relying on a single device in the data center, the Management VPC should have redundant VPN connections established through multiple customer gateways. This will ensure high availability and fault tolerance in case one of the VPN connections or customer gateways fails.

**Question 63**
**A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2**

**instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.**
**A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.**

**Which change to the network architecture should a solutions architect recommend to meet this requirement?**

A. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.

B. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.

C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets. **Correct answer**

D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

**Overall explanation**
Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

To meet the requirement of ensuring that network traffic for file transfers does not go over the internet, you should move the EC2 instances to private subnets and create a VPC endpoint for Amazon S3. The VPC endpoint allows your EC2 instances to access S3 privately, without going over the internet. Linking the VPC endpoint to the route table for the private subnets ensures that the traffic flows through the endpoint for secure and private communication with Amazon S3. This approach effectively isolates the traffic from the public internet while still allowing your instances to access S3.

**Question 64**
**A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.**

**Which set of services should a solutions architect recommend to meet these requirements?**

A. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage

B. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage

C. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage **Correct answer**

D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

**Overall explanation**

- Use Amazon EBS for maximum performance, as it provides high I/O performance, and it's a suitable choice for video processing with 10 TB of storage.
- Use Amazon S3 for durable data storage with 300 TB, which is ideal for storing media content.
- Use Amazon S3 Glacier for archival storage with 900 TB of data that is not in use anymore.

**Question 65**
**A company has an AWS Glue extract, transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket. New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.**
**What should the solutions architect do to prevent AWS Glue from reprocessing old**

**data?**

A. Edit the job by setting the NumberOfWorkers field to 1.

B. Edit the job to delete data after the data is processed.

C. Use a FindMatches machine learning (ML) transform.

D. Edit the job to use job bookmarks. **Correct answer**

**Overall explanation**
Edit the job to use job bookmarks.

Job bookmarks are used in AWS Glue to track the last-processed data and are particularly useful when dealing with data that is continuously added to, such as in your scenario with new XML data added to the S3 bucket every day. By enabling job bookmarks, AWS Glue will keep track of the last-processed data, allowing subsequent job runs to pick up from where the previous run left off. This prevents the reprocessing of old data, improving the efficiency of your ETL job.

**Question 66**
**A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The company wants to optimize the costs to run the job.**

**Which solution will meet these requirements?**

**A.** Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.

**B.** Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.

C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.

D. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour. **Correct answer**

**Overall explanation**

Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.

- AWS Lambda is a suitable service for running periodic tasks.
- The code is small, runs infrequently, and AWS Lambda offers a cost-effective solution for such scenarios.

**Question 67**

**A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.**

**Which combination of steps should a solutions architect take to accomplish this? (Choose two.)**

A. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.

B. Configure a VPC gateway endpoint for Amazon S3 within the VPC. **Correct selection**

C. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

D. Create a bucket policy to make the objects in the S3 bucket public.

E. Create a bucket policy that limits access to only the application tier running in the VPC. **Correct selection**

**Overall explanation**

To provide secure access to an Amazon S3 bucket from Amazon EC2 instances inside a VPC, you should take the following steps:

1. Configure a VPC endpoint for Amazon S3 (S3 gateway endpoint) within the VPC . This allows the EC2 instances to access Amazon S3 securely without using public internet routing.
2. Create a bucket policy that limits access to only the application tier running in the VPC. This policy should specify the allowed VPC and specific EC2 instance security group(s) or IP addresses that should have access to the S3 bucket.

**Question 68**

**A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.**

**Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)**

- **A.** Use AWS Shield Advanced to stop the DDoS attack. **Correct selection**
- **B.** Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.
- **C.** Configure Amazon GuardDuty to automatically block the attackers.
- **D.** Configure the website to use Amazon CloudFront for both static and dynamic content. **Correct selection**
- **E.** Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.

**Overall explanation**
Use AWS Shield Advanced to stop the DDoS attack.

Configure the website to use Amazon CloudFront for both static and dynamic content.

AWS Shield Advanced provides additional protection against large-scale DDoS attacks, including infrastructure and application layer attacks. This service can help protect your website from DDoS attacks that originate from thousands of IP addresses.

Amazon CloudFront can help distribute the traffic to your website and provide protection by acting as a Content Delivery Network (CDN). It can also provide DDoS protection by absorbing and mitigating attack traffic, as it has built-in DDoS protections. By using CloudFront for both static and dynamic content, you can improve the performance and security of your website.

**Question 69**
**A company has a three-tier web application that is in a single server. The company wants to migrate the application to the AWS Cloud. The company also wants the application to align with the AWS Well-Architected Framework and to be consistent with AWS recommended best practices for security, scalability, and resiliency.**

**Which combination of solutions will meet these requirements? (Choose three.)**

A. Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.**Correct selection**

B. Set up security groups and network access control lists (network ACLs) to control access to the database layer. Set up a single Amazon RDS database in a private subnet.

C. Create a VPC across two Availability Zones with the application's existing architecture. Host the application with existing architecture on an Amazon EC2 instance in a private subnet in each Availability Zone with EC2 Auto Scaling groups. Secure the EC2 instance with security groups and network access control lists (network ACLs).

D. Use a single Amazon RDS database. Allow database access only from the application tier security group.

E. Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups. **Correct selection**

F. Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups. **Correct selection**

**Overall explanation**

Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.

Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups.

Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups.

**Explanation:**

1. VPC Across Two Availability Zones : Aligns with the AWS Well-Architected Framework's best practice of designing for fault tolerance and high availability. Distributing resources across multiple Availability Zones enhances resiliency.
2. Elastic Load Balancers (: Provides a scalable and fault-tolerant architecture. Distributing traffic with load balancers ensures that the application remains available and responsive.
3. Amazon RDS Multi-AZ Cluster : Ensures high availability and fault tolerance for the database tier. Multi-AZ deployment replicates the database across different Availability Zones, reducing the risk of downtime.

4. Private Subnets: Hosting each tier in private subnets enhances security by preventing direct access from the internet and enforcing a more controlled and secure architecture.
5. Auto Scaling Groups (: Ensures that the web and application tiers can scale horizontally based on demand, providing scalability and efficient resource utilization.

**Question 70**

**A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.**

**Which design should the solutions architect use?**

A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.

C. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.

**D.** Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application.

Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue. **Correct answer**

**Overall explanation**

Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.

Amazon SQS (Simple Queue Service) is designed for decoupling applications and provides a durable way to store messages (job items). You can have the Auto Scaling group scale based on the number of items in the SQS queue. When there are more messages to be processed, it will automatically add more nodes to handle the workload, and when the queue is empty, it can remove excess nodes. This allows the application to run in parallel and efficiently handle varying workloads.

**Question 71**

**A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently.**

**Which solution meets these requirements?**

A. **Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.**

B. **Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager. Correct answer**

C. **Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.**

D. **Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.**

**Overall explanation**

Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

**Here's why this option is suitable:**

1. AWS Secrets Manager: AWS Secrets Manager is specifically designed for securely storing, managing, and rotating sensitive information like database credentials. It provides automatic rotation options, ensuring that credentials are frequently updated without manual intervention. It's a best practice for handling sensitive data securely.
2. IAM Permissions: You can grant IAM permissions to your web servers to access Secrets Manager securely. This allows your web servers to retrieve the database credentials when needed, but these credentials remain protected and can be rotated automatically as required.

This option aligns with security best practices and ensures that your database credentials are managed in a secure and automated manner, meeting both the security and credential rotation requirements.

**Question 72**

**A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.**

**What should the solutions architect recommend?**

A. Use Amazon CloudFront with a custom origin pointing to the on-premises servers. **Correct answer**

B. Move the website to Amazon S3. Use Cross-Region Replication between Regions.

C. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.

D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers.

**Overall explanation**

To optimize site loading times for new European users while keeping the site's backend in the United States, you should use a Content Delivery Network (CDN). In this case, Amazon CloudFront is a suitable solution as it provides low-latency content delivery globally. It caches your website's content in edge locations in Europe and serves it to users from the nearest edge location, reducing latency.

Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

With this configuration, your website content will be cached in CloudFront's edge locations across Europe, improving the site's loading times for European users. This is a quick and effective way to achieve the desired optimization without migrating your website to an EC2 instance or S3, and it's suitable for immediate deployment before the product launch.

**Question 73**

**A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.**

**What should a solutions architect do to meet this requirement?**

A. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application

B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region

C. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer

D. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer **Correct answer**

**Overall explanation**

Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer:

- Multi-AZ EC2 Auto Scaling: This provides high availability by distributing EC2 instances across multiple Availability Zones.
- Application Load Balancer: Distributes incoming application traffic across multiple EC2 instances.

This solution aligns with the requirement for ensuring the application is highly available by leveraging Multi-AZ EC2 Auto Scaling and an Application Load Balancer.

**Question 74**

**A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.**

**Which solution will meet this requirement with the LEAST operational overhead?**

A. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

C. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

**D.** Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery streams sources. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination. **Correct answer**

**Overall explanation**

Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream's source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.

With this approach, you can configure CloudWatch Logs to deliver log data to the Kinesis Data Firehose delivery stream, and Kinesis Data Firehose will efficiently load the data into Amazon OpenSearch Service without the need for manual intervention or custom code. This minimizes operational overhead and ensures near-real-time log delivery to Amazon OpenSearch Service.

**Question 75**

**A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.**
**Which architecture offers the HIGHEST availability?**

**A.** Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.

**B.** Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled. **Correct answer**

C. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

**Overall explanation**

Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

This architecture provides the highest availability by utilizing Amazon MQ's active/standby broker configuration across multiple Availability Zones, having an Auto Scaling group for the consumer EC2 instances in multiple Availability Zones, and enabling Amazon RDS for MySQL with Multi-AZ. These measures ensure redundancy, fault tolerance, and high availability for the message processing system with low operational complexity.

**Question 76**

**A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.**

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

A. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.

B. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts. **Correct answer**

C. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.

**D.** Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.

**Overall explanation**

Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.

**Explanation:**

1. Lake Formation Tag-Based Access Control: It allows for fine-grained access control using tags, reducing the operational overhead associated with manual permission management.
2. Cross-Account Permissions: Lake Formation supports cross-account access, enabling the secure sharing of data between accounts.
3. Least Operational Overhead: Compared to copying data or managing permissions individually, tag-based access control simplifies data sharing and access management.
4. Fine-Grained Control: Tag-based access control provides fine-grained control over who can access specific datasets based on tags.
5. Integration with Lake Formation: Leveraging Lake Formation's capabilities ensures a seamless and well-integrated solution for data lake management.

**Question 77**

**A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.**

**Which solution can the company use to route traffic to all the EC2 instances?**

A. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups. **Correct answer**

B. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution’s origin.

C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

D. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution’s origin.

**Overall explanation**

- AWS Global Accelerator is a service that provides static IP addresses and routes traffic over the AWS global network to a specific set of endpoints. It optimizes the global routing of traffic to your resources and provides high availability and fault tolerance.
- By creating a standard accelerator in AWS Global Accelerator, you can route traffic to both NLBs in us-west-2 and eu-west-1 Regions.
- Endpoint groups allow you to group resources together and define the traffic routing to those resources. In this case, you would create two endpoint groups, one for us-west-2 and one for eu-west-1.
- You can add the two NLBs as endpoints for their respective endpoint groups, allowing traffic to be directed to the NLBs in both Regions.

This solution provides improved performance and availability by utilizing AWS Global Accelerator's global network and efficient routing of traffic to the appropriate NLBs in different Regions. It simplifies the DNS routing configuration and helps ensure high availability and low latency for users in the United States and Europe.

**Question 78**

**An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple**

**Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.**

**Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.**

**What should the solutions architect do to resolve this issue with the LEAST operational overhead?**

A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.

B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.

C. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

D. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout. **Correct answer**

**Overall explanation**

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

**Question 79**

**A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.**

**Which solution will meet these requirements with the LEAST amount of administrative effort?**

A. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules. **Correct answer**

B. Set up AWS Shield in bath Regions. Associate Regional web ACLs with an API stage.

C. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.

D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

**Overall explanation**

AWS Firewall Manager is a managed service that makes it easier to centrally configure and manage AWS WAF (Web Application Firewall) rules across multiple accounts and resources. By using AWS Firewall Manager, you can create and maintain a set of AWS WAF rules centrally and ensure consistent protection for your API Gateway in both the us-east-1 and ap-southeast-2 Regions.

This option minimizes administrative effort by allowing you to manage the AWS WAF rules from a centralized location, making it easier to apply consistent security controls across multiple Regions and accounts.

**Question 80**

**A company wants to securely exchange data between its software as a service (SaaS) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account.**

**A.** Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3. **Correct answer**

**B.** Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.

**C.** Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.

**D.** Create an AWS Step Functions workflow. Define the task to transfer the data securely from Salesforce to Amazon S3.

**Overall explanation**

Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.

- Amazon AppFlow is designed for securely transferring data between AWS services and SaaS applications.
- It supports encryption in transit and integrates with AWS KMS for data encryption.

**Question 81**

**A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased. The company wants to accommodate the larger workload without adding infrastructure.**

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

A. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.

B. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger. **Correct answer**

C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.

D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.

**Overall explanation**

Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.

**Explanation:**

1. Reserved DB Instances: Buying reserved instances is a cost-effective strategy for predictable workloads. It provides a significant discount compared to on-demand pricing.
2. Making RDS Instance Larger: Increasing the size of the existing Amazon RDS for PostgreSQL DB instance allows it to handle a larger workload without adding infrastructure.
3. Cost-Effective Scaling: This solution leverages the cost efficiency of reserved instances while scaling vertically to accommodate the increased workload.
4. Operational Simplicity: Scaling vertically by modifying the instance size is operationally simpler than introducing additional instances or complex architectural changes.
5. Meeting Increased Workload: By combining reserved instances and vertical scaling, this solution efficiently meets the requirement of handling a larger workload without significant additional infrastructure.

**Question 82**

**A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability 10 delete the objects.**

**What should a solutions architect do to meet these requirements?**

**A.** Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

**B.** Create an S3 bucket. Use AWS CloudTrail to track any S3 API events that modify the objects. Upon notification, restore the modified objects from any backup versions that the company has.

**C.** Create an S3 Glacier vault. Apply a write-once, read-many (WORM) vault lock policy to the objects.

**D.** Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket’s default retention mode for new objects. **Correct answer**

**Overall explanation**

Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket’s default retention mode for new objects.

This option leverages S3 Object Lock, which is designed to prevent the deletion or modification of objects for a specified retention period. By enabling versioning, you ensure that new versions of objects are created when changes are made, while the original versions remain unchangeable based on the retention settings. Setting a 100-year retention period effectively makes the objects unchangeable for a long duration. By using governance mode as the default retention mode, it allows you to establish the retention requirements without changing existing objects, thus meeting the company's requirement to prevent data from being changed. Users who need to delete the objects can be granted permissions to bypass the retention period if necessary.

**Question 83**

**A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.**

**Which solution will meet these requirements?**

**A.** Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

**B.** Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years. **Correct answer**

**C.** Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.

**D.** Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.

**Overall explanation**

Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.

This option specifies transitioning objects to the S3 Glacier Deep Archive storage class after 2 years, which aligns with your requirement to keep data for at least 25 years. It allows you to reduce storage costs significantly by moving objects to a more cost-effective storage class while ensuring data retention.

This Option focuses on transitioning the data to the Glacier Deep Archive storage class after the initial 2 years, and it doesn't impact the immediate availability of the most recent data. This approach is cost-effective for long-term data retention, and it maintains data availability for the first 2 years, meeting your requirements.

**Question 84**

**A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.**

**A solutions architect needs to design a solution that stores customer data that is created during database upgrades.**

**Which solution will meet these requirements?**

**A.** Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.

**B.** Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database. **Correct answer**

**C.** Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.

**D.** Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.

**Overall explanation**

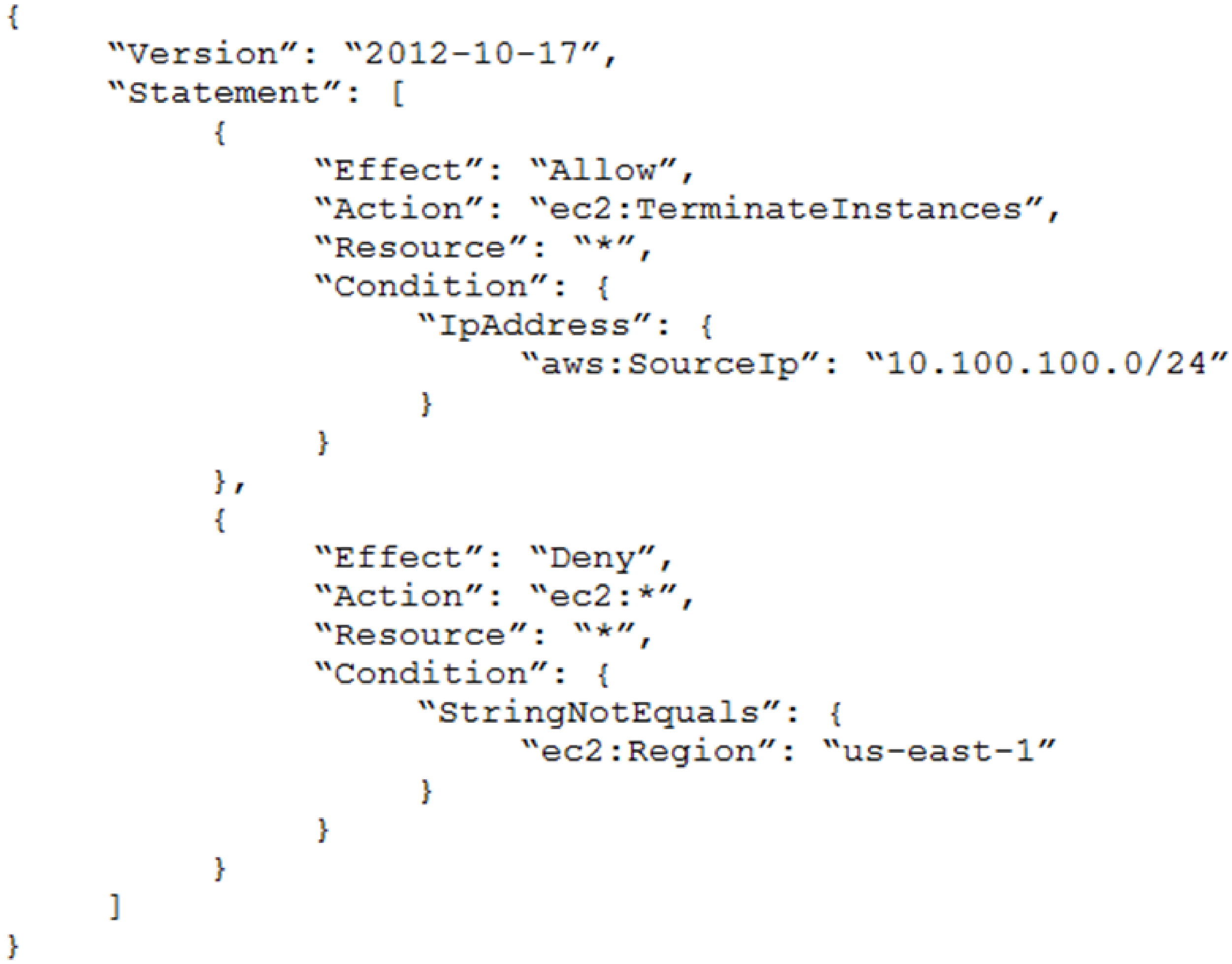
Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

**Here's why this option is suitable:**

1. Amazon SQS FIFO Queue: Using an Amazon SQS FIFO queue provides a reliable and ordered way to store customer data, ensuring data integrity and preventing data loss during database upgrades. FIFO queues guarantee that messages are processed in the exact order they are received, and they can also handle multiple consumers without losing data.
2. Decoupling and Scalability: Storing data in an SQS queue decouples the database write operation from the Lambda functions, allowing the Lambda functions to continue operating without interruptions during database upgrades. It also provides an asynchronous and scalable way to handle the data, making it easier to manage surges in incoming data.
3. Lambda Function: You can create a dedicated Lambda function to poll the SQS queue and store the customer data in the database. This Lambda function can be configured to operate efficiently and handle the data transfer without interruptions.

**Question 85**

**An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:**



```
{
     “Version”: “2012-10-17”,
     “Statement”: [
          {
               “Effect”: “Allow”,
               “Action”: “ec2:TerminateInstances”,
               “Resource”: “*”,
               “Condition”: {
                    “IpAddress”: {
                         “aws:SourceIp”: “10.100.100.0/24”
                    }
               }
          },
          {
               “Effect”: “Deny”,
               “Action”: “ec2:*”,
               “Resource”: “*”,
               “Condition”: {
                    “StringNotEquals”: {
                         “ec2:Region”: “us-east-1”
                    }
               }
          }
     ]
}
```

- **A.** Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- **B.** Users can terminate an EC2 instance in any AWS Region except us-east-1.
- **C.** Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- **D.** Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254. **Correct answer**

**Overall explanation**
1. Allow termination of any instance if user’s source IP address is 100.100.254.

2. Deny termination of instances that are not in the us-east-1 Combining this two, you get: “Allow instance termination in the us-east-1 region if the user’s source IP address is 10.100.100.254. Deny termination operation on other regions.”

**Question 86**
**A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years.**
**What is the MOST operationally efficient solution that meets these requirements?**

- **A.** Use AWS Backup to create backup schedules and retention policies for the table.
  **Correct answer**
- **B.** Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
- **C.** Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
- **D.** Use DynamoDB point-in-time recovery to back up the table continuously.

**Overall explanation**
Use AWS Backup to create backup schedules and retention policies for the table.

AWS Backup is a fully managed backup service that simplifies the process of creating and managing backups of AWS resources, including Amazon DynamoDB tables. By using AWS Backup, you can easily create backup schedules and retention policies to ensure your data is retained for the required duration without the need for custom scripts or manual processes. This approach simplifies data retention management, ensuring that backups are created and retained as needed for the specified 7-year period.

**Question 87**
**A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.**

**An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.**

**What should the solutions architect do to maximize reliability of the application's infrastructure?**

A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.

B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.**Correct answer**

C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.

D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances Update the DB instance to be Multi-AZ, and enable deletion protection.

**Overall explanation**

**Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.**

**Explanation:**

1. Multi-AZ Deployment for RDS: Provides high availability by replicating the database instance to another Availability Zone, minimizing downtime.
2. Deletion Protection: Enabling deletion protection for the DB instance prevents accidental deletion, adding a layer of security.
3. EC2 Auto Scaling Across Zones: Running EC2 instances in an Auto Scaling group across multiple Availability Zones enhances availability and fault tolerance.
4. Application Load Balancer (ALB): Distributes incoming traffic across multiple EC2 instances, ensuring that the application remains available even if one instance fails.
5. Overall Redundancy: Combining Multi-AZ RDS, deletion protection, EC2 Auto Scaling, and ALB enhances the overall reliability of the application.

**Question 88**

**A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.**
**The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.**

**Which solution meets these requirements?**

- **A.** Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

- **B.** Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.

**C.** Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.

**D.** Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB. **Correct answer**

**Overall explanation**

Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.

This solution leverages AWS Lambda to process the photos, which allows for on-demand scaling based on the number of incoming requests and concurrent users. You can use Amazon DynamoDB to store both the photos and metadata, ensuring that the database can handle varying levels of traffic without manual scaling or additional infrastructure management. This approach aligns with the serverless architecture principles, reducing operational overhead and providing a scalable solution for the growing user base.

**Question 89**

**A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.**

**Which solution will meet these requirements with the LEAST operational effort?**

**A.** Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database. **Correct answer**

**B.** Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.

**C.** Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

**D.** Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.

**Overall explanation**
Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.

Here's why this option is the best choice:

1. Multi-AZ for RDS: Configuring the Amazon Aurora PostgreSQL database as Multi-AZ ensures high availability within the same region. It provides automatic failover to a standby database instance in case the primary instance becomes unavailable. This minimizes downtime and data loss in the event of a failure.
2. RDS Proxy: Amazon RDS Proxy is a fully managed database proxy service that allows you to distribute read and write database traffic across multiple database instances. It provides connection pooling, failover, and read/write splitting capabilities, improving the overall reliability and performance of database connections.
3. Auto Scaling Across Multiple Availability Zones: Configuring the Auto Scaling group to use multiple Availability Zones ensures that your EC2 instances are distributed across different data centers, enhancing fault tolerance and reducing the risk of application downtime.

**Question 90**
**A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.**

**Which solution meets these requirements?**

A. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.

B. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option. **Correct answer**

C. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

**D.** Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.

**Overall explanation**

Convert the existing database instance to a Multi-AZ deployment:

- Multi-AZ deployment provides high availability by automatically replicating the primary database to a standby instance in another Availability Zone.
- It does not require changes to the application code, as it is a managed service feature of RDS.
- In the event of a failure, RDS automatically fails over to the standby instance.

This solution aligns with the requirement to minimize database downtime without changes to the application code.

**Question 91**

**A company is implementing a shared storage solution for a gaming application that is hosted in an on-premises data center. 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 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.

B. 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**

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 EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.

**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.

Amazon FSx for Lustre is a fully managed service that provides high-performance file storage for Lustre workloads. It supports Lustre clients, making it a suitable solution for the company's requirements to use Lustre clients to access data. This choice provides a fully managed solution and is optimized for high-performance requirements.

**Question 92**
**A company runs applications on Amazon EC2 instances in one AWS Region. The company wants to back up the EC2 instances to a second Region. The company also wants to provision EC2 resources in the second Region and manage the EC2 instances centrally from one AWS account.**

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

A. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances. **Correct answer**

B. Deploy a similar number of EC2 instances in the second Region. Use AWS DataSync to transfer the data from the source Region to the second Region.

C. Create a disaster recovery (DR) plan that has a similar number of EC2 instances in the second Region. Configure data replication.

D. Create point-in-time Amazon Elastic Block Store (Amazon EBS) snapshots of the EC2 instances. Copy the snapshots to the second Region periodically.

**Overall explanation**

Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.

- AWS Backup provides a centralized backup solution, and configuring cross-Region backup ensures redundancy and disaster recovery capabilities.

**Question 93**

**A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.**

**The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition ofAmazon Aurora to host the DB instance.**

**Which solutions will create the new DB instance? (Choose two.)**

A. Import the RDS snapshot directly into Aurora. **Correct selection**

B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.

C. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.

E. Upload the database dump to Amazon S3. Then import the database dump into Aurora. **Correct selection**

**Overall explanation**

Import the RDS snapshot directly into Aurora.

Upload the database dump to Amazon S3. Then import the database dump into Aurora.

**Explanation:**

1. Import RDS Snapshot into Aurora: Amazon Aurora supports direct import of RDS snapshots, making it a seamless process to create a new Aurora instance from an RDS snapshot.
2. Upload Database Dump to Amazon S3 and Import into Aurora: Uploading the database dump to Amazon S3 and then importing it into Aurora is a valid approach for creating a new Aurora instance, providing flexibility.

**Question 94**

**A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.**

**What should the solutions architect do to meet these requirements?**

A. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.

B. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails. **Correct answer**

C. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.

D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

**Overall explanation**

Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.

**Here's why this option is suitable:**

1. AWS Direct Connect: Direct Connect provides dedicated network connections from your on-premises data center to AWS. It offers a private and consistent network connection with low latency and high reliability. This is an ideal choice for primary connectivity.
2. VPN Connection: A VPN (Virtual Private Network) connection can serve as a cost-effective backup solution. In the event of a primary Direct Connect connection failure, the VPN connection can take over. While VPN connections may have higher latency compared to Direct Connect, they can provide a good level of redundancy.

This combination ensures consistent low-latency connectivity through the primary Direct Connect connection and automatic failover to a VPN connection if the primary connection fails, providing high availability while minimizing costs.

**Question 95**

**A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.**

**Which solution will meet these requirements?**

A. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.

B. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

C. Configure the Requester Pays feature on the company's S3 bucket. **Correct answer**

D. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.

**Overall explanation**

Configure the Requester Pays feature on the company's S3 bucket.

By enabling Requester Pays, the marketing firm (or any other requesters) will be responsible for covering the data transfer costs when accessing objects in the company's S3 bucket. This ensures that the company is not billed for data transfer costs incurred by external parties. It allows the marketing firm to access the data in the bucket while being charged for the associated data transfer fees.

This solution helps the survey company minimize its data transfer costs and allows the marketing firm to pay for their own usage of the data.

**Question 96**

**A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.**

**What should the solutions architect recommend to meet these requirements?**

- **A.** Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
- **B.** Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
- **C.** Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.
- **D.** Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time. **Correct answer**

**Overall explanation**

The best solution to meet the RPO and RTO requirements would be to use DynamoDB point-in-time recovery (PITR). This feature allows you to restore your DynamoDB table to any point in time within the last 35 days, with a granularity of seconds. To recover data within a 15-minute RPO, you would simply restore the table to the desired point in time within the last 35 days. To meet the RTO requirement of 1 hour, you can use the DynamoDB console, AWS CLI, or the AWS SDKs to enable PITR on your table. Once enabled, PITR continuously captures point-in-time copies of your table data in an S3 bucket. You can then use these point-in-time copies to restore your table to any point in time within the retention period.

**Question 97**
**A company uses AWS Organizations. The company wants to operate some of its AWS accounts with different budgets. The company wants to receive alerts and automatically prevent provisioning of additional resources on AWS accounts when the allocated budget threshold is met during a specific period.**

**Which combination of solutions will meet these requirements? (Choose three.)**

A. Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.**Correct selection**

B. Use AWS Budgets to create a budget. Set the budget amount under the Billing dashboards of the required AWS accounts.

C. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.**Correct selection**

D. Create an IAM role for AWS Budgets to run budget actions with the required permissions.**Correct selection**

E. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate config rule to prevent provisioning of additional resources.

F. Create an IAM user for AWS Budgets to run budget actions with the required permissions.

**Overall explanation**

Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.

- AWS Budgets is used to create budgets and set budget amounts for specific accounts.

Create an IAM role for AWS Budgets to run budget actions with the required permissions.

- An IAM role is required to allow AWS Budgets to take actions based on budget thresholds.

Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

- Using alerts and budget actions, combined with an IAM identity and SCP, provides a comprehensive solution to control spending.

**Question 98**

**A company uses AWS Organizations to run workloads within multiple AWS accounts. A tagging policy adds department tags to AWS resources when the company creates tags.**

**An accounting team needs to determine spending on Amazon EC2 consumption. The accounting team must determine which departments are responsible for the costs regardless ofAWS account. The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer.**

**Which solution meets these requirements in the MOST operationally efficient way?**

A. From the Organizations member account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by the tag name, and filter by EC2.

B. From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2. **Correct answer**

C. From the Organizations management account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

D. From the Organizations member account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

**Overall explanation**

From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

- Activating a user-defined cost allocation tag at the management account level allows for consistent tagging across all member accounts.
- Creating a cost report in Cost Explorer allows the accounting team to analyze costs based on the specified tag.

**Question 99**

**A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection.**

**After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window.**

**Which solution will meet these requirements?**

A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task Start the transfer to an Amazon S3 bucket. **Correct answer**

B. Use rsync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.

C. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

D. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

**Overall explanation**

Create an AWS DataSync agent in the corporate data center. Create a data transfer task. Start the transfer to an Amazon S3 bucket.

**Explanation:**

1. **AWS DataSync**: Efficiently and securely transfers large amounts of data between on-premises storage and Amazon S3.
2. **Data Transfer Task**: AWS DataSync allows the creation of data transfer tasks to move data from on-premises to Amazon S3 seamlessly.
3. **Minimal Disruption**: The transfer can be performed without disrupting access to or updates of the data during the migration window.
4. **Efficient Transfer**: AWS DataSync optimizes data transfer over the Direct Connect connection, ensuring efficient use of available bandwidth.
5. **S3 Integration**: DataSync can transfer data directly to an Amazon S3 bucket, making it suitable for large-scale data migrations.

**Question 100**

**A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.**

**What is the MOST secure way for the company to share the database with the auditor?**

A. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key. **Correct answer**

B. Create a read replica of the database. Configure IAM standard database authentication to grant the auditor access.

C. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.

D. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the S3 bucket.

**Overall explanation**

The most secure way for the company to share the database with the auditor is, Create an encrypted snapshot of the database, share the snapshot with the auditor, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

By creating an encrypted snapshot, the company ensures that the database data is protected at rest. Sharing the encrypted snapshot with the auditor allows them to have their own copy of the database securely.

In addition, granting access to the AWS KMS encryption key ensures that the auditor has the necessary permissions to decrypt and access the encrypted snapshot.

This allows the auditor to restore the snapshot and access the data securely. This approach provides both data protection and access control, ensuring that the database is securely shared with the auditor while maintaining the confidentiality and integrity of the data.

**Question 101**

**A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.**

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

**A.** Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests.

**B.** Use a high performance computing (HPC) solution such as AWS ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

**C.** Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.

**D.** Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests. **Correct answer**

**Overall explanation**

Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.

This solution allows you to run your containerized web application in a managed, serverless environment using AWS Fargate, which requires minimal code changes. Service Auto Scaling ensures that your application can handle varying levels of incoming requests, and using an Application Load Balancer enables you to distribute the traffic efficiently. This option minimizes operational overhead and requires fewer code changes compared to other solutions.

**Question 102**
**An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible. Data processing will require 1 GB of memory and will finish within 30 seconds.**

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

A. Use Amazon EMR with an Apache Spark script

B. Use AWS Lambda with a Python script **Correct answer**

C. Use AWS Glue with a PySpark job

D. Use AWS Glue with a Scala job

**Overall explanation**
Use AWS Lambda with a Python script:

- AWS Lambda is a cost-effective, serverless compute service that automatically scales based on demand.
- Python is a supported language for AWS Lambda, providing flexibility in scripting and data processing.
- Since the data processing requirement is small (1 GB of memory, 30 seconds), AWS Lambda is suitable for this scenario.
- AWS Lambda functions can be triggered by events, such as data uploads to the S3 bucket, making it a good fit for real-time processing.

Using AWS Lambda with a Python script is a cost-effective and efficient solution for the given requirements.

**Question 103**
**A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier**

**consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.**

**How should security groups be configured in this situation? (Choose two.)**

A. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier. **Correct selection**

B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.

C. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

D. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. **Correct selection**

E. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.

**Overall explanation**

Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.

**Explanation:**

- This option allows inbound traffic on port 443 (HTTPS) from any IP address (0.0.0.0/0).
- Port 443 is commonly used for secure web traffic, so this rule would enable incoming HTTPS requests to the web tier from anywhere on the internet.
- It's important to note that allowing inbound traffic from 0.0.0.0/0 means that the web tier is accessible over HTTPS from any source IP, which might be a security concern. It should be used with caution, and access should be restricted to trusted sources if possible.

Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.

**Explanation:**

- This option allows inbound traffic on port 1433 (the default port for Microsoft SQL Server) from the security group associated with the web tier's EC2 instances.
- It establishes a secure connection between the web tier and the database tier by allowing traffic only from instances associated with the web tier's security group.
- This configuration is highly secure as it restricts incoming database connections to only instances in the web tier, which is the intended access pattern for a two-tier web application. It follows the principle of least privilege.

**Question 104**

**A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.**

**Which action meets these requirements for storing and retrieving location data?**

A. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

B. Use Amazon Athena with Amazon S3.

C. Use Amazon QuickSight with Amazon Redshift.

D. Use Amazon API Gateway with AWS Lambda. **Correct answer**

**Overall explanation**

Use Amazon API Gateway with AWS Lambda.

Using Amazon API Gateway with AWS Lambda is a suitable option for building a REST API to store and retrieve location data. AWS Lambda can handle the backend logic for storing and retrieving the data, and Amazon API Gateway can serve as the front end for the REST API, making it accessible for the bicycle sharing company's applications. This option is well-suited for building a multi-tier architecture to support the requirements.

**Question 105**
**A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.**

**Which solution will meet these requirements?**

- **A.** Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- **B.** Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach **Correct answer**
- **C.** Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- **D.** Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

**Overall explanation**
Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone.