**COHORT 3**

**AWS SOLUTIONS ARCHITECT ASSOCIATE**

**PRACTICE QUESTIONS 3**

**105 QUESTIONS**

**Question 1  
A company hosts a three-tier web application in the AWS Cloud. A Multi-AZAmazon RDS for MySQL server forms the database layer Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database. The data in the cache must always match the data in the database.  
  
Which solution will meet these requirements?**

1. Implement the write-through caching strategy **Correct answer**
2. Implement the lazy loading caching strategy
3. Implement the adding TTL caching strategy
4. Implement the AWS AppConfig caching strategy

**Overall explanation**

Implement the write-through caching strategy:

* In a write-through caching strategy, data is written to the cache and the underlying database simultaneously.
* This ensures that the data in the cache always matches the data in the database, meeting the requirement stated in the question.
* This strategy helps maintain consistency between the cache and the database.

**Question 2  
A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing, and the company is concerned about a potential increase in cost.**

1. Create an Amazon CloudFront distribution to cache state files at edge locations**Correct answer**
2. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files
3. Create a second ALB in an alternative AWS Region. Route user traffic to the closest Region to minimize data transfer costs
4. Create an Amazon ElastiCache cluster. Connect the ALB to the ElastiCache cluster to serve cached files

**Overall explanation**

Create an Amazon CloudFront distribution to cache static files at edge locations:

* Amazon CloudFront is a content delivery network (CDN) service that caches static content at edge locations.
* By using CloudFront, you can offload traffic from your EC2 instances and reduce the load on your ALB, leading to potential cost savings.

**Question 3**

**A security team wants to limit access to specific services or actions in all of the team’s AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.  
  
What should a solutions architect do to accomplish this?**

1. Create a service control policy in the root organizational unit to deny access to the services or actions Correct answer
2. Create cross-account roles in each account to deny access to the services or actions.
3. Create an ACL to provide access to the services or actions.
4. Create a security group to allow accounts and attach it to user groups.

**Overall explanation**

To limit access to specific services or actions in all AWS accounts within an organization in AWS Organizations while providing a scalable and centralized way to manage permissions, you should:

Create a service control policy in the root organizational unit to deny access to the services or actions.

Here's why this is the appropriate choice:

* Service Control Policies (SCPs) are a feature in AWS Organizations that allow you to set fine-grained permissions and access controls at the organizational level. SCPs allow you to specify which AWS services and actions are allowed or denied for member accounts within the organization.
* By creating a single SCP at the root organizational unit, you can centrally control access to specific services or actions across all AWS accounts in the organization. This provides a scalable and unified approach to managing permissions and ensuring consistent security policies.
* SCPs are a robust way to enforce and manage security policies across multiple AWS accounts within an organization. They allow you to deny access to specific services or actions while permitting others, thus providing a centralized point of control.

Using SCPs is a best practice for managing access control at the organization level and ensures that the security policies are consistently applied across all accounts, making it easier to maintain and scale security policies.

**Question 4**

**A company needs to connect several VPCs in the us-east-1 Region that span hundreds of AWS accounts. The company's networking team has its own AWS account to manage the cloud network.  
  
What is the MOST operationally efficient solution to connect the VPCs?**

1. Set up VPC peering connections between each VPC. Update each associated subnet’s route table
2. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team’s AWS account to connect to each VPC.
3. Create an AWS Transit Gateway in the networking team’s AWS account. Configure static routes from each VPC. Correct answer
4. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet

**Overall explanation**

Create an AWS Transit Gateway in the networking team’s AWS account. Configure static routes from each VPC.

* AWS Transit Gateway simplifies connectivity between multiple VPCs, making it operationally efficient.

**Question 5**

**A company wants to migrate its existing on-premises monolithic application to AWS. The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.  
  
Which solution will meet these requirements?**

1. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
2. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.
3. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
4. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target. Correct answer

**Overall explanation**

Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

Explanation:

1. Amazon Elastic Container Service (Amazon ECS): Amazon ECS is a fully managed container orchestration service that allows you to run Docker containers on AWS. It provides a scalable and efficient way to manage and run containerized applications.
2. Application Load Balancer: The Application Load Balancer (ALB) is part of AWS Elastic Load Balancing and is designed for distributing incoming application traffic across multiple targets, such as Amazon ECS containers.

This approach offers more control over the infrastructure compared to a serverless architecture. It's suitable for scenarios where you want to maintain some aspects of the backend code, possibly when migrating a monolithic application that's already containerized or where containers offer specific benefits. However, it also comes with more operational overhead since you need to manage and scale the containers yourself.

**Question 6**

**A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region.**

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

1. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS). Use Amazon Athena to query the data. Correct answer
2. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
3. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.
4. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.

**Overall explanation**

Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon Athena to query the data.

Here's why this option is the best fit:

1. New S3 Bucket: Creating a new S3 bucket helps isolate the existing data from the new data and changes, providing a clear separation for the serverless solution.
2. S3 Cross-Region Replication (CRR): Replicating encrypted objects to an S3 bucket in another Region satisfies the requirement for data replication to a different AWS Region.
3. Server-side Encryption with AWS KMS multi-Region keys (SSE-KMS): Using multi-Region AWS KMS keys for server-side encryption ensures data security and encryption in transit between Regions. It simplifies key management while meeting encryption requirements.
4. Amazon Athena for Querying Data: Amazon Athena is a serverless query service for analyzing data stored in Amazon S3. It allows you to run SQL queries on your data without having to manage servers, making it a suitable choice for serverless data analysis.

**Question 7**

**A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.  
  
Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)**

1. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode. Correct selection
2. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.
3. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.
4. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation. Correct selection
5. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.

**Overall explanation**

Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.  
  
Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation.

**Question 8**

**A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilizalion metrics are spiking when monthly reports run.  
  
What is the MOST cost-effective solution?**

1. Increase the Provisioned IOPS on the Aurora instance.
2. Migrate the monthly reporting to Amazon Redshift.
3. Migrate the Aurora database to a larger instance class.
4. Migrate the monthly reporting to an Aurora Replica. Correct answer

**Overall explanation**

Migrate the monthly reporting to an Aurora Replica.

Explanation:

1. Amazon Aurora Replicas: Amazon Aurora allows you to create read replicas that offload read traffic from the primary database instance. Read replicas share the same underlying data volume as the primary instance but provide additional read capacity. By running the monthly reporting on an Aurora Replica, you can alleviate the performance impact on the primary instance.
2. Cost-Effectiveness: This approach is cost-effective because it doesn't require migrating to a completely different database service like Redshift, which might incur additional costs and operational complexity. It also doesn't involve scaling up the primary instance or increasing Provisioned IOPS, which can be more costly.

By using an Aurora Replica for reporting, you can maintain good performance for your ecommerce application without significant additional costs.

**Question 9**

**A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.  
What should the solutions architect do to meet these requirements?**

1. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
2. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.
3. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
4. Create Amazon CloudWatch composite alarms where possible. Correct answer

**Overall explanation**

Create Amazon CloudWatch composite alarms where possible:

* Amazon CloudWatch composite alarms allow you to create alarms based on the combination of multiple metrics and conditions. You can use composite alarms to address situations where both CPU utilization and read IOPS need to be considered together. This approach is valid if you find it effective in reducing false alarms and providing the necessary control.

**Question 10Skipped**

**A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2 instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.  
  
In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.  
  
Which solutions will meet these requirements with the LEAST administrative effort? (Choose two.)**

1. Create backup vaults in us-west-1 and in us-west-2 by using AWS Backup. Create a backup plan for the EC2 instances based on tag values. Create an AWS Lambda function to run as a scheduled job to copy the backup data to us-west-2.
2. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region. Correct selection
3. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily. Correct selection
4. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Copy the image on demand.
5. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Specify the backup schedule to run twice daily. Copy on demand to us-west-2.

**Overall explanation**

Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region.

* Using AMI lifecycle policies with AWS Backup simplifies automated backups, and copying to another region ensures disaster recovery.

Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily.

* It leverages AWS Backup to define a backup plan that runs twice daily and copies backups to us-west-2. AWS Backup automates EC2 instance backups.  
    
  Together, these options provide automated, regional EC2 backup capabilities with minimal administrative overhead.

**Question 11**

**A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.  
  
What should the solutions architect do to accomplish this?**

1. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.
2. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations. Correct answer
3. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
4. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.

**Overall explanation**

Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.

Explanation:

This option is based on a serverless architecture, which is ideal for scalable and elastic solutions. Here's why it's the best choice:

* Amazon API Gateway is designed to create and manage RESTful APIs. It can seamlessly integrate with AWS Lambda functions, making it easy to build a serverless API.
* AWS Lambda is a serverless compute service that can be automatically scaled to handle any number of requests. It only runs when needed, which is a cost-effective way to handle occasional spikes in demand, such as during the holiday season.
* By using API Gateway to pass requests to Lambda for tax computations, you can ensure that your API remains responsive, even during high-demand periods, and you only pay for the compute resources when requests are being processed.

This serverless approach provides the scalability and elasticity required for handling variable workloads efficiently. It's also cost-effective, as you won't be paying for idle resources during periods of lower activity.

**Question 12**

**A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.**

**Which solutions will meet these requirements? (Choose two.)**

1. Use rules in AWS WAF to prevent internet access. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
2. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
3. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3. Correct selection
4. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3. Correct selection
5. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

**Overall explanation**

Create Amazon CloudWatch composite alarms where possible:

* Amazon CloudWatch composite alarms allow you to create alarms based on the combination of multiple metrics and conditions. In this case, you can create a composite alarm that combines both CPU utilization and read IOPS to trigger an alarm only when both conditions are met simultaneously. This approach can help reduce false alarms, as it ensures that the alarm is triggered when both criteria (CPU utilization > 50% and high read IOPS) are met at the same time. It's a suitable solution for addressing the specific requirement of acting when both conditions occur together.

Create Amazon CloudWatch Synthetics canaries to monitor the application:

* Amazon CloudWatch Synthetics enables you to create "canaries," which are configurable scripts that run on a schedule to monitor your application's endpoints and functionality. You can use Synthetics to create scripted checks that include not only CPU utilization but also the specific conditions or metrics you need to monitor. This approach allows you to perform more complex checks and take action based on custom criteria. It can be an effective solution for monitoring and acting upon specific behaviors or thresholds, including CPU utilization and read IOPS in your application.

**Question 13**

**A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.  
  
Which solution will meet these requirements MOST cost-effectively?**

1. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
2. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic. Correct answer
3. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.
4. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.

**Overall explanation**

Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.

* A VPC gateway endpoint for S3 allows private communication without using a NAT gateway, reducing data transfer costs.

**Question 14**

**A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.  
  
What should the solutions architect do to meet this requirement?**

1. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance. Correct answer
2. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.
3. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.
4. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.

**Overall explanation**

This option, which involves creating an IAM role and assigning it to the EC2 instance, is not the most secure approach for managing sensitive credentials in AWS Systems Manager Parameter Store.

Assigning an IAM role to an EC2 instance gives it a set of permissions that are defined by the role. In the case of securely storing and retrieving sensitive data like database credentials, it's generally recommended to create a specific IAM policy that grants read access to the Parameter Store parameter and allows decrypt access to the associated AWS Key Management Service (KMS) key. This approach provides fine-grained control and is considered a more secure method.

**Question 15**

**A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should.be protected throughout the entire application stack, and access to the information should be restricted to certain applications.  
  
Which action should the solutions architect take?**

1. Configure a CloudFront field-level encryption profile. Correct answer
2. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.
3. Configure a CloudFront signed cookie.
4. Configure a CloudFront signed URL.

**Overall explanation**

Configure a CloudFront field-level encryption profile.

Explanation:

Field-level encryption is the most appropriate solution when you need to secure sensitive data submitted by users throughout your application stack and restrict access to that information. Field-level encryption ensures that data is encrypted at the edge by CloudFront and remains encrypted until it reaches your backend servers, protecting it during transmission.

**Question 16**

**A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.  
  
The company’s developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).  
  
What should a solutions architect recommend for communication between the microservices?**

1. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.
2. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.
3. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue. Correct answer
4. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.

**Overall explanation**

Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.

Using Amazon SQS allows you to decouple the communication between microservices. Data producers send messages to an SQS queue, and data consumers process these messages. This approach provides flexibility, scalability, and resilience as the microservices can process messages at their own rate, and it can handle high traffic efficiently. This is a common pattern in microservices architectures for asynchronous communication.

**Question 17**

**A company seeks a storage solution for its application. The solution must be highly available and scalable. The solution also must function as a file system, be mountable by multiple Linux instances in AWS and on premises through native protocols, and have no minimum size requirements. The company has set up a Site-to-Site VPN for access from its on-premises network to its VPC.  
  
Which storage solution meets these requirements?**

1. Amazon FSx Multi-AZ deployments
2. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes
3. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points
4. Amazon Elastic File System (Amazon EFS) with multiple mount targets Correct answer

**Overall explanation**

Amazon Elastic File System (Amazon EFS) with multiple mount targets:

* EFS provides scalable, highly available file storage that can be mounted by multiple Linux instances.
* Using multiple mount targets allows access from AWS and on-premises through native protocols.

**Question 18**

**A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.  
  
Which solutions meet these requirements? (Choose two.)**

1. Create an Amazon RDS DB instance in Multi-AZ mode. Correct selection
2. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load. Correct selection
3. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.
4. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
5. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.

**Overall explanation**

Create an Amazon RDS DB instance in Multi-AZ mode. (This provides automatic failover and high availability for the database.)

Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load. (Fargate is a serverless compute engine for containers, which means you don't need to manage the underlying EC2 instances, making it more hands-off.)

These choices will help ensure high availability and reduced manual intervention for the ecommerce application.

**Question 19**

**A company has an ordering application that stores customer information in Amazon RDS for MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.  
  
What should a solutions architect do to meet these requirements?**

1. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
2. Schedule the reporting queries for non-peak hours.
3. Create a read replica. Move reporting queries to the read replica. Correct answer
4. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.

**Overall explanation**

By creating a read replica of the Amazon RDS for MySQL database, you can offload reporting queries to the read replica, which can help eliminate timeouts during order processing on the primary database. Read replicas are designed for read-heavy workloads and can provide additional capacity for running reporting queries without affecting the performance of the primary database.

**Question 20**

**A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.**

**Which action should the company take to meet these requirements MOST cost-effectively?**

1. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.
2. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.
3. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days. Correct answer
4. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.

**Overall explanation**

To meet the requirements while optimizing storage costs for ringtones that are infrequently accessed after 90 days, you should implement an S3 Lifecycle policy that moves objects to a less expensive storage class after 90 days. So, the correct answer is:

D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-IA (S3 Standard-Infrequent Access) after 90 days.

Here's the reasoning:

1. Initially, you can store the ringtones in Amazon S3 Standard, which is designed for frequently accessed data and offers low latency.
2. After the 90-day period, when downloads for older ringtones are infrequent, you can use an S3 Lifecycle policy to automatically transition these objects to a less expensive storage class, such as S3 Standard-IA. S3 Standard-IA is more cost-effective for data that is accessed less frequently, and it can help you save on storage costs.

By implementing this policy, you ensure that you retain access to the most recently accessed ringtones in S3 Standard while moving older, less frequently accessed ringtones to the more cost-effective S3 Standard-IA storage class. This approach allows you to meet the cost-saving requirements without sacrificing user access to recently accessed files.

**Question 21**

**A company has Amazon EC2 instances that run nightly batch jobs to process data. The EC2 instances run in an Auto Scaling group that uses On-Demand billing. If a job fails on one instance, another instance will reprocess the job. The batch jobs run between 12:00 AM and 06:00 AM local time every day.  
  
Which solution will provide EC2 instances to meet these requirements MOST cost-effectively?**

1. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses.
2. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.
3. Create a new launch template for the Auto Scaling group. Set the instances to Spot Instances. Set a policy to scale out based on CPU usage. Correct answer
4. Create a new launch template for the Auto Scaling group. Increase the instance size. Set a policy to scale out based on CPU usage.

**Overall explanation**

Create a new launch template for the Auto Scaling group. Set the instances to Spot Instances. Set a policy to scale out based on CPU usage.

* Using Spot Instances with Auto Scaling based on CPU usage is a cost-effective and scalable solution for batch jobs.

**Question 22**

**A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.  
  
Which architecture should the solutions architect choose that provides high availability?**

1. Create an Auto Scaling group that uses three instances across each of two Regions.
2. Modify the Auto Scaling group to use three instances across each of two Availability Zones. Correct answer
3. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
4. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

**Overall explanation**

Modify the Auto Scaling group to use three instances across each of two Availability Zones.

Explanation:

To achieve high availability for the application, you should distribute your resources across multiple Availability Zones (AZs) within a single AWS Region. By using multiple AZs, you ensure that if one AZ becomes unavailable, your application can continue running in the other AZ. In this scenario, modifying the Auto Scaling group to use three instances across each of two Availability Zones is the appropriate choice.

Here's why this option is the best approach:

1. High Availability: Spreading your web servers across multiple Availability Zones increases fault tolerance. If one AZ experiences issues or failures, the instances in the other AZ can continue to handle traffic.
2. Load Balancing: With an Application Load Balancer (ALB), you can easily distribute incoming traffic evenly across instances in multiple AZs. This further enhances the high availability of your application.
3. Scalability: Auto Scaling groups provide scalability, ensuring that you have the right number of instances available to handle your application's traffic load.
4. Resilience: In case an instance becomes unhealthy or fails, the Auto Scaling group replaces it with a new one, maintaining application availability.

Using multiple AZs is a fundamental practice for achieving high availability on AWS without modifying the application itself. It's a recommended approach for maintaining the reliability and fault tolerance of your infrastructure.

**Question 23**

**A company’s web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.  
  
Which configuration will meet this requirement?**

1. Configure the security group for the EC2 instances.
2. Configure AWS WAF on the Application Load Balancer in a VPC. Correct answer
3. Configure the network ACL for the subnet that contains the EC2 instances.
4. Configure the security group on the Application Load Balancer.

**Overall explanation**

To restrict access to a web application hosted on Amazon EC2 instances to be accessible from a specific country, you should use AWS WAF (Web Application Firewall) along with the Application Load Balancer (ALB) in a VPC. AWS WAF allows you to create rules that specify conditions for allowing or denying access based on various factors, including the geographic location of the requester, which is what you need to fulfill this requirement.

Here's how to configure it:

Configure AWS WAF on the Application Load Balancer in a VPC.

Explanation:

* AWS WAF allows you to create a web access control list (web ACL) that defines rules for allowing or blocking web requests based on various conditions, including the country or region from which the request is originating.
* You can associate this AWS WAF web ACL with your Application Load Balancer (ALB) in your VPC. This will enable AWS WAF to inspect incoming web requests and block any requests that do not meet the defined criteria, such as requests originating from outside the specific country.
* This approach provides a more targeted and flexible way to restrict access to your application based on geographic location while allowing legitimate traffic to reach your EC2 instances behind the ALB.

**Question 24**

**A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.  
  
What should the company do to obtain access to customer accounts in the MOST secure way?**

1. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.
2. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.
3. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.
4. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company’s account. Correct answer

**Overall explanation**

By having customers create an IAM role with the necessary permissions in their own accounts, the company can use AWS Identity and Access Management (IAM) to establish cross-account access.

The trust policy allows the company's AWS account to assume the customer's IAM role temporarily, granting access to the specified resources (EC2 instances and CloudWatch metrics) within the customer's account.

This approach follows the principle of least privilege, as the company only requests the necessary permissions and does not require long-term access keys or user credentials from the customers.

**Question 25**

**A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.  
  
How should a solutions architect design the application to ensure the LEAST amount of latency for all users?**

1. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.
2. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin. Correct answer
3. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
4. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.

**Overall explanation**

Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.

Explanation:

* In this solution, the entire application stack is deployed in a single AWS Region, which simplifies the architecture and reduces operational complexity.
* Amazon CloudFront is a Content Delivery Network (CDN) service that caches and serves static content from edge locations around the world. By specifying the ALB (Application Load Balancer) as an origin, CloudFront can distribute content to users globally.
* CloudFront caches static content, such as images, CSS, and JavaScript files, at its edge locations. This ensures that users receive these static resources from a location geographically closer to them, reducing latency.

**Question 26**

**Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.  
  
Which action should the solutions architect take to accomplish this?**

1. Use Amazon CloudFront with the S3 bucket as its origin. Correct answer
2. Generate presigned URLs for the files.
3. Use the geoproximity feature of Amazon Route 53.
4. Use cross-Region replication to all Regions.

**Overall explanation**

To efficiently and effectively serve static HTML pages stored in an Amazon S3 bucket to users around the world, the recommended solution is to use Amazon CloudFront, which is content delivery network (CDN) service. Therefore, the correct option is:

Use Amazon CloudFront with the S3 bucket as its origin.

Here's why Amazon CloudFront is the right choice:

1. Global Content Delivery: Amazon CloudFront has a network of edge locations worldwide, enabling it to cache and deliver content to users from the nearest edge location. This reduces latency and ensures fast access for users from around the world.
2. High Availability: CloudFront enhances the availability of your content by distributing it across multiple edge locations. This helps in handling high traffic and provides failover in case of issues with specific edge locations.
3. Security: Amazon CloudFront supports SSL/TLS for secure delivery of content. It also provides DDoS protection with AWS Shield.
4. Scalability: CloudFront scales automatically to handle varying levels of traffic, making it suitable for events that may generate millions of views.
5. Cost-Efficiency: CloudFront helps reduce the load on your origin (S3 bucket in this case) by caching content at edge locations. This can lead to cost savings in terms of reduced data transfer costs and reduced load on the origin.

In summary, using Amazon CloudFront as a content delivery network in front of the Amazon S3 bucket is the optimal choice to efficiently serve static HTML pages for a global audience.

**Question 27**

**A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.  
  
Which capability should the solutions architect use to meet the compliance requirements?**

1. VPC endpoint Correct answer
2. AWS Key Management Service (AWS KMS)
3. Private subnet
4. Virtual private gateway

**Overall explanation**

**VPC endpoint:**

* **A VPC endpoint allows you to privately connect your VPC to supported AWS services, including Amazon S3, without requiring public internet access.**
* **This ensures that traffic between EC2 instances and S3 remains within the AWS network and doesn't traverse the public internet.**

**Question 28**

**An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.**What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

1. Use a VPC endpoint for DynamoDB. Correct answer
2. Use a NAT gateway in a public subnet.
3. Use the internet gateway attached to the VPC.
4. Use a NAT instance in a private subnet.

**Overall explanation**

Use a VPC endpoint for DynamoDB.

Explanation:

The most secure way to access an Amazon DynamoDB table from Amazon EC2 instances in private subnets while ensuring that the traffic does not leave the AWS network is to use a VPC endpoint for DynamoDB. Here's why:

1. VPC Endpoints: A VPC endpoint allows you to privately connect your VPC to supported AWS services like DynamoDB without the need for an internet gateway, NAT gateway, or NAT instance. It keeps the traffic within the AWS network and does not traverse the public internet.
2. Security: Using a VPC endpoint provides a more secure connection as it doesn't rely on public internet access. It also eliminates the need to configure complex network address translation (NAT) gateways or instances.
3. Simplicity: It is a simpler and more direct method of accessing DynamoDB without exposing your resources to the internet. This reduces the attack surface and ensures that the traffic remains within your VPC.

**Question 29**

**A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.  
What should a solutions architect do to meet these requirements?**

1. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules. Correct answer
2. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
3. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.
4. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.

**Overall explanation**

Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules.

Here's how this approach works:

1. You can create two AWS Lambda functions, one to start the DB instance and another to stop it. These Lambda functions will interact with the Amazon RDS service to perform these actions.
2. Configure Amazon EventBridge (formerly known as CloudWatch Events) scheduled rules to trigger these Lambda functions at specific times. You can set up rules to start the DB instance before it's needed and stop it after the required 12-hour period. EventBridge allows you to create cron-like expressions to schedule these events.
3. Configure the Lambda functions as event targets for the rules. This ensures that the specified Lambda function is executed when the scheduled time arrives.

By automating the start and stop of the DB instance, you can ensure that it's available when required and inactive during the times when it's not in use, effectively minimizing costs. This is a cost-effective and efficient way to manage your RDS instance for a part-time use case.

**Question 30**

**A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application’s database. The database must be highly available and must fail over automatically if a disruptive event occurs.  
  
Which solution will meet these requirements?**

1. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.
2. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.
3. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication. Correct answer
4. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.

**Overall explanation**

Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.

This solution provides high availability within the same AWS Region by deploying database instances in separate Availability Zones. Setting up database replication between these instances allows for automatic failover. In the event of a failure in one Availability Zone, the application can fail over to the database in the other Availability Zone. This approach provides both high availability and automatic failover, meeting the specified requirements.

**Question 31**

**A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object. The company needs to retain only the two most recent versions of the pictures. The company wants to reduce costs. The company has identified the S3 bucket as a large expense.  
  
Which solution will reduce the S3 costs with the LEAST operational overhead?**

1. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions. Correct answer
2. Deactivate versioning on the S3 bucket and retain the two most recent versions.
3. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions.
4. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions.

**Overall explanation**

Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.

* S3 Lifecycle policies can be configured to automatically manage object versions and retain the desired number of versions.

**Question 32**

**A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3 bucket. The company will store new data directly in Amazon S3.  
  
Which solution will meet these requirements with the LEAST operational overhead?**

1. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket
2. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket Correct answer
3. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket
4. Use AWS Snowball to move the data to an S3 bucket

**Overall explanation**

AWS DataSync is a fully managed data transfer service that simplifies and automates the process of moving data between on-premises storage and Amazon S3. It provides secure and efficient data transfer with built-in encryption, ensuring that the data is encrypted in transit.

By using AWS DataSync, the company can easily migrate the 100 GB of historical data from their on-premises location to an S3 bucket. DataSync will handle the encryption of data in transit and ensure secure transfer.

**Question 33**

**A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed: If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.  
  
Which solution meets these requirements and is the MOST operationally efficient?**

1. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
2. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.
3. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process. Correct answer
4. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).

**Overall explanation**

Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.

Here's why:

1. Amazon SQS: Amazon SQS is a managed message queuing service that efficiently decouples the sender and receiver applications. It can handle the throughput of 1,000 messages per hour without any issues.
2. Dead-Letter Queue: Amazon SQS allows you to set up a dead-letter queue to collect messages that failed to process. This ensures that failed messages don't impact the processing of remaining messages, and you can easily investigate and reprocess them separately.
3. Operational Efficiency: Amazon SQS is fully managed, meaning you don't need to provision or manage servers or databases like in the case of Redis . It's also simpler to set up and manage than Kinesis and SNS for this use case.

This option provides a scalable, reliable, and operationally efficient solution for decoupling the sender and processor applications and handling messages between them.

**Question 34**

**A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.  
  
Which solution will meet these requirements?**

1. Place the JSON documents in an Amazon S3 bucket. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in an Amazon Aurora DB cluster.
2. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages. Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type. Use the container to process the SQS messages. Store the results on an Amazon RDS DB instance.
3. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster. Correct answer
4. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume. Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances. Run the Python code on the EC2 instances to process the documents. Store the results on an Amazon RDS DB instance.

**Overall explanation**

1. It leverages Amazon S3 for storing JSON documents, which is a scalable and durable object storage service.
2. It uses AWS Lambda to process documents as they arrive in the S3 bucket. AWS Lambda automatically scales based on the incoming workload, and you don't need to manage the underlying infrastructure.
3. It stores the results in an Amazon Aurora DB cluster, which is a fully managed relational database service. This combination provides high availability, scalability, and minimal operational overhead.

This option allows you to focus on the application code and business logic, as AWS Lambda takes care of the infrastructure management and scaling, making it a cost-effective and efficient solution.

**Question 35**

**A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.  
The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.  
  
What should a solutions architect do to meet these requirements with the LEAST operational overhead?**

1. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
2. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
3. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule. Correct answer
4. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.

**Overall explanation**

To meet the requirements of moving files automatically from the initial S3 bucket to the analysis S3 bucket and running Lambda functions on the copied data, with the least operational overhead, you should choose option B:

Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Here's why this is the recommended approach:

1. By using a Lambda function to copy files from the initial S3 bucket to the analysis S3 bucket, you can control the copy process and apply custom logic if needed.
2. Configuring the analysis S3 bucket to send event notifications to Amazon EventBridge (CloudWatch Events) allows you to react to new file arrivals.
3. Creating an ObjectCreated rule in EventBridge (CloudWatch Events) with Lambda and SageMaker Pipelines as targets enables you to execute Lambda functions and trigger SageMaker Pipelines whenever new files are created in the analysis S3 bucket. This is a flexible and scalable solution to automate the process.

**Question 36**

**A company’s order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.  
  
What should a solutions architect do to meet these requirements?**

1. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB). Update the order system to send messages to the ALB endpoint.
2. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function, and subscribe the function to the SNS topic. Configure the order system to send messages to the SNS topic. Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.
3. Move the EC2 instances into an Auto Scaling group. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
4. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue. Correct answer

**Overall explanation**

Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.

This solution introduces an Amazon SQS queue, which acts as a buffer for the order messages. The EC2 instances in the Auto Scaling group can consume messages from the queue. If the system experiences a failure, messages are not lost but are held in the queue, allowing for automatic recovery and processing when the system is operational again. This approach provides both resilience and the ability to automatically process orders if a system outage occurs.

**Question 37**

**A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.  
  
Which solution meets these requirements?**

1. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.
2. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
3. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data. Correct answer
4. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.

**Overall explanation**

Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.

Amazon RDS (Relational Database Service) with Multi-AZ (Availability Zone) functionality provides synchronous replication across multiple nodes in separate Availability Zones. This ensures data durability and high availability. In case of a failure, the standby node in another Availability Zone can take over quickly, minimizing data loss.

**Question 38**

**A company’s infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.  
  
Which solution will meet these requirements with the LEAST operational overhead?**

1. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region. Correct answer
2. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.
3. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.
4. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.

**Overall explanation**

Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.

Explanation:

AWS Backup is a fully managed backup service that simplifies the creation, management, and retention of backups across various AWS services. When it comes to creating backups in a separate Region with the least operational overhead, AWS Backup is an ideal choice for the following reasons:

1. Fully Managed: AWS Backup is a fully managed service, meaning it handles all aspects of backup management for various AWS services, including EC2 instances and RDS databases. This reduces operational overhead and simplifies backup operations.
2. Cross-Region Backup: AWS Backup provides the capability to create cross-Region backups, allowing you to replicate backups to a separate Region, which meets the requirement to back up data in a separate Region.
3. Simplified Management: AWS Backup offers a centralized and consistent way to manage backups across different AWS services. You can easily configure backup policies and retention settings.
4. EC2 and RDS Support: AWS Backup supports both EC2 instances and RDS databases, making it a suitable choice for your infrastructure, which includes EC2 instances and an RDS DB instance.

**Question 39**

**A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS. The solutions architect has decided to create IAM groups. The solutions architect will add the new users to IAM groups based on department.  
  
Which additional action is the MOST secure way to grant permissions to the new users?**

1. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions
2. Create IAM roles that have least privilege permission. Attach the roles to the IAM groups
3. Apply service control policies (SCPs) to manage access permissions
4. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups Correct answer

**Overall explanation**

An IAM policy is an object in AWS that, when associated with an identity or resource, defines their permissions. Permissions in the policies determine whether a request is allowed or denied. You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources.

**Question 40**

**A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.  
  
What should the solutions architect do to meet this requirement?**

1. Enable AWS Shield Advanced to prevent attacks. Correct answer
2. Configure Amazon Macie to prevent attacks.
3. Configure Amazon GuardDuty to monitor the ALB.
4. Add an Amazon Inspector agent to the ALB.

**Overall explanation**

To reduce the risk of Distributed Denial of Service (DDoS) attacks against a public web application that uses an Application Load Balancer (ALB), you should:

Enable AWS Shield Advanced to prevent attacks.

Here's why this is the appropriate choice:

* AWS Shield Advanced is a managed Distributed Denial of Service (DDoS) protection service that provides comprehensive protection against large and sophisticated DDoS attacks. It is designed to safeguard AWS resources, including ALBs, from various types of DDoS attacks.
* AWS Shield Advanced includes features like real-time attack visibility, protection against network and application layer DDoS attacks, and access to the AWS DDoS Response Team (DRT) for assistance during attacks.
* AWS Shield Advanced is specifically designed to help prevent and mitigate DDoS attacks, making it a robust choice to enhance the security of your public web application and protect it from such threats.

Configuring AWS Shield Advanced on your ALB helps ensure the availability and reliability of your application by proactively mitigating DDoS attacks, which is a crucial security measure for web applications.

**Question 41**

**A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.  
  
Which method should the solutions architect select?**

1. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.
2. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint. Correct answer
3. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
4. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.

**Overall explanation**

Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint:

* DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that can significantly improve read performance.
* DAX is designed to require minimal application changes, making it an optimal solution for low-latency access to DynamoDB.

**Question 42**

**A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.  
How should a solutions architect accomplish this?**

1. **Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.**
2. **Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.**
3. **Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.**
4. **Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue. Correct answer**

**Overall explanation**

Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.

Explanation:

In this scenario, where the order of processing is important, using an Amazon SQS FIFO (First-In-First-Out) queue is the appropriate choice. FIFO queues are designed to maintain the order of messages and are ideal when you need to process messages sequentially in the order they were sent.

Here's how this solution works:

1. Event data is produced and sent to the Amazon SQS FIFO queue, ensuring that the order is maintained.
2. An AWS Lambda function is set up to process messages from the queue. AWS Lambda is a serverless compute service that can automatically scale and run your code in response to events. It's a good choice for processing events or messages as they are received.
3. The Lambda function can process each message in the queue in the exact order they were received, ensuring the specific order of processing is maintained.

This solution minimizes operational overhead because you don't have to manage the underlying infrastructure, and it ensures that messages are processed in the desired order.

**Question 43**

**A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.  
The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.  
  
Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)**

1. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
2. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.
3. Purchase a 1-year Compute Savings Plan for the front end and API layer. Correct selection
4. Use Spot Instances for the data ingestion layer. Correct selection
5. Use On-Demand Instances for the data ingestion layer

**Overall explanation**

Use Spot Instances for the data ingestion layer:

* Spot Instances are a cost-effective option for workloads that can be interrupted or have flexible start and end times, which seems to be the case for the sporadic and unpredictable data ingestion layer.
* Spot Instances provide significant cost savings compared to On-Demand Instances, making them a suitable choice when costs need to be optimized.
* You can set a maximum price for Spot Instances, and they will be terminated if the current spot price rises above that maximum. This allows you to control costs and ensure that interruptions are acceptable for this workload.

Purchase a 1-year Compute Savings Plan for the front end and API layer:

* AWS Savings Plans provide cost savings for a commitment to usage, making them a cost-effective choice for predictable and stable workloads, such as the front end and API layer, where usage can be forecasted over a year.
* By purchasing a 1-year Compute Savings Plan, you are locking in lower prices for your front end and API workloads, helping you save on your AWS bill compared to using On-Demand Instances.

By combining Spot Instances for the unpredictable data ingestion layer and a 1-year Compute Savings Plan for the predictable front end and API layer, you are effectively optimizing costs based on the unique characteristics and demands of each component in your architecture. This approach ensures that you get the most cost-effective solution while meeting your application's requirements.

**Question 44**

**A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.  
  
Which solution will meet these requirements?**

1. **Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the c**onnection with another AWS account.
2. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS account.
3. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.
4. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console. Correct answer

**Overall explanation**

Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.

* Downsizing the Direct Connect connection to 200 Mbps meets the requirement of minimizing costs without compromising security.

**Question 45**

**A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.  
Which solution will meet these requirements?**

1. Use S3 Object Lock in governance mode with a legal hold of 1 year.
2. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added. Configure the function to track the hash of the saved object so that modified objects can be marked accordingly.
3. Use S3 Object Lock in compliance mode with a retention period of 365 days. Correct answer
4. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket. Use an S3 bucket policy to only allow the IAM role.

**Overall explanation**

To meet the requirements of allowing a few scientists to add new files while restricting all other users from modifying or deleting files in the repository and retaining each file for a minimum of 1 year, you should use S3 Object Lock in compliance mode with a retention period of 365 days. So, the correct answer is:

Use S3 Object Lock in compliance mode with a retention period of 365 days.

Here's the reasoning:

1. S3 Object Lock in compliance mode ensures that objects in your S3 bucket are protected against deletion or modification for the specified retention period. This satisfies the requirement of retaining each file for a minimum of 1 year.
2. By setting the retention period to 365 days, you fulfill the requirement for retaining files for at least 1 year after their creation date.
3. You can also use IAM policies to grant specific scientists the necessary permissions to add new files to the S3 bucket while restricting all other users to read-only access. This way, only the authorized scientists can modify the content of the S3 bucket.

**Question 46**

**A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.  
Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.  
  
What should the solutions architect recommend to meet this requirement?**

1. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources. Correct answer
2. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
3. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
4. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.

**Overall explanation**

Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

* Modifying the network ACL provides an efficient way to block traffic before it reaches the instances.

**Question 47**

**A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.  
  
Which solution will meet these requirements?**

1. Containerize the web application. Deploy the web application to Amazon EC2 instances. Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.
2. Create an Amazon S3 bucket. Enable static web hosting on the S3 bucket. Upload the static content to the S3 bucket. Use AWS Lambda to process all dynamic content.
3. Deploy the web application to Amazon EC2 instances that are configured with Java and PHP. Use Auto Scaling groups and an Application Load Balancer to manage the website’s availability.
4. Deploy the web application to an AWS Elastic Beanstalk environment. Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing. Correct answer

**Overall explanation**

Deploy the web application to an AWS Elastic Beanstalk environment. Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing.

Explanation:

AWS Elastic Beanstalk is a Platform as a Service (PaaS) offering that provides an easy and managed way to deploy and run web applications. It supports multiple languages and platforms, including Java and PHP. With Elastic Beanstalk, you can easily create multiple environments for testing new site features without the need for significant operational overhead.

URL swapping allows you to route traffic between different environments, making it a suitable choice for feature testing and ensuring high availability. This approach offers flexibility, ease of use, and scalability while minimizing operational complexity.

**Question 48**

**An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.  
  
What should a solutions architect recommend to meet this requirement?**

1. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.
2. Use Amazon ElastiCache for Redis.
3. Replicate data by using DynamoDB global tables.
4. Use Amazon DynamoDB Accelerator (DAX). Correct answer

**Overall explanation**

Use Amazon DynamoDB Accelerator (DAX).

Explanation:

To improve the performance efficiency of Amazon DynamoDB without reconfiguring the application and without adding significant operational overhead, you should recommend using Amazon DynamoDB Accelerator (DAX). Here's why:

1. DAX Caching: Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB. It provides microsecond response times for read-intensive DynamoDB workloads by caching frequently accessed data.
2. No Application Changes: DAX is designed to be a drop-in caching solution for DynamoDB. You can enable it for your DynamoDB tables without modifying your application code. Your application continues to interact with DynamoDB using the same API calls.
3. Fully Managed: DAX is fully managed, which means you don't need to handle operational overhead. AWS takes care of the provisioning, management, and scaling of DAX clusters.
4. Significant Performance Improvement: DAX can significantly reduce the read latency for DynamoDB, making it an ideal solution for read-intensive workloads, such as those involving media metadata.

The other options, such as using Amazon ElastiCache for Redis, DynamoDB global tables, or Amazon ElastiCache for Memcached, do not offer the same level of seamless integration with DynamoDB or are not specifically designed for improving DynamoDB read performance without application changes.

**Question 49Skipped**

**A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).  
Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)**

1. Use Amazon Kinesis Data Analytics for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
2. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format. Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters.
3. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster.
4. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load the data into Amazon S3 in Apache Parquet format. Correct selection
5. Use Amazon Athena for one-time queries. Use Amazon QuickSight to create dashboards for KPIs. Correct selection

**Overall explanation**

To meet the requirements of consolidating data from different sources, processing incoming data, and staging it in different Amazon S3 buckets for business analytics, while minimizing operational overhead, you can follow these steps:

1. Use AWS Glue for ETL (Extract, Transform, Load):
   * Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load it into Amazon S3 in Apache Parquet format. This approach simplifies the data preparation process and is a recommended practice for data lake architectures. It helps in processing, transforming, and storing data efficiently in a structured format.
2. Use Amazon Athena for one-time queries and Amazon QuickSight for creating dashboards:
   * Use Amazon Athena for one-time queries and Amazon QuickSight to create dashboards for KPIs. Amazon Athena is a serverless, interactive query service that can query data stored in S3, including the data ingested using AWS Glue. Amazon QuickSight is a business intelligence tool that can visualize and explore your data for creating KPI dashboards.

**Question 50**

**A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.**

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

1. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
2. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
3. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission. Correct answer
4. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.

**Overall explanation**

To meet the requirement of not allowing direct navigation to the S3 URL and serving the files through an Amazon CloudFront distribution, you should use an Origin Access Identity (OAI). Here's how you can do it:

Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

By using an OAI, you restrict access to your S3 bucket directly and allow access only through the CloudFront distribution, ensuring that users cannot access the files via the S3 URL.

**Question 51**

**A company wants to ingest customer payment data into the company's data lake in Amazon S3. The company receives payment data every minute on average. The company wants to analyze the payment data in real time. Then the company wants to ingest the data into the data lake.  
  
Which solution will meet these requirements with the MOST operational efficiency?**

1. Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time. Correct answer
2. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
3. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.
4. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.

**Overall explanation**

Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.

* Amazon Kinesis Data Firehose simplifies the process of ingesting data into Amazon S3, and it can deliver data to other destinations, including Kinesis Data Analytics.
* Amazon Kinesis Data Analytics can analyze streaming data in real time.

**Question 52**

**A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.  
  
Which solution will meet these requirements?**

1. Enable S3 Transfer Acceleration for the S3 bucket
2. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC
3. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC Correct answer
4. Enable S3 Intelligent-Tiering for the S3 bucket

**Overall explanation**

Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC:

* A VPC endpoint for Amazon S3 enables you to access Amazon S3 from your VPC without using an internet gateway or a VPN connection.
* This ensures that traffic stays within the AWS network, minimizing costs and preventing internet traversal.

**Question 53**

**An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.  
  
Which solution meets these requirements MOST cost-effectively?**

1. Amazon RDS for PostgreSQL
2. Amazon OpenSearch Service (Amazon Elasticsearch Service)
3. Amazon S3 Glacier
4. Amazon S3 Standard Correct answer

**Overall explanation**

For a disaster recovery solution that provides fast access to the data, keeps the data for 30 days, and is cost-effective, Amazon S3 is a suitable option. Amazon S3 offers different storage classes, and for this scenario, you can use the Amazon S3 Standard storage class. This class provides low-latency access to your data, making it accessible in milliseconds if needed.

So, the option that meets the requirements MOST cost-effectively is Amazon S3 Standard.

**Question 54**

**An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts, and the application did not process the orders of those customers.  
  
A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.  
  
Which solution will meet these requirements?**

1. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint. Correct answer
2. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.
3. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.
4. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

**Overall explanation**

Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.

Explanation:

To address the issue of high CPU and memory utilization on the database due to a large number of open connections and to prevent timeout errors in the application, you can use Amazon RDS Proxy. Here's why this solution is the best choice:

1. Scalability: Amazon RDS Proxy is designed to efficiently manage database connections and distribute them evenly to the database. This helps reduce the number of open connections and prevents the database from getting overwhelmed during traffic surges.
2. Connection Pools: RDS Proxy maintains a connection pool, which allows it to reuse database connections and share them among clients. This reduces the overhead of creating and closing connections for each request.
3. Lambda Integration: You can easily modify the Lambda function to use the RDS Proxy endpoint instead of the direct database endpoint. This change doesn't require significant modifications to the application code.
4. Improved Database Performance: By offloading connection management to RDS Proxy, you can ensure that the database can handle more incoming requests without the need for major changes to the database itself.
5. Global Availability: RDS Proxy also supports multi-AZ deployments, making it a robust and highly available solution for managing database connections.

Overall, using Amazon RDS Proxy is the recommended approach for optimizing database connections, improving performance, and preventing timeout errors without the need for significant changes to the application code.

**Question 55**

**A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files. A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.  
  
Which solution will meet these requirements?**

1. Launch an Amazon EC2 instance in a private subnet in a VPInstruct the new partner to upload files to the EC2 instance by using a VPN. Run a cron job script, on the EC2 instance to upload files to the S3 data lake.
2. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint. Choose the S3 data lake as the destination. Correct answer
3. Use Amazon S3 File Gateway as an SFTP server. Expose the S3 File Gateway endpoint URL to the new partner. Share the S3 File Gateway endpoint with the new partner.
4. Launch Amazon EC2 instances in a private subnet in a VPC. Place a Network Load Balancer (NLB) in front of the EC2 instances. Create an SFTP listener port for the NLB. Share the NLB hostname with the new partner. Run a cron job script on the EC2 instances to upload files to the S3 data lake.

**Overall explanation**

Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint. Choose the S3 data lake as the destination.

With AWS Transfer Family, you can set up a fully managed SFTP service that provides a highly available SFTP server with minimal operational overhead. It's integrated with Amazon S3, so the files uploaded via SFTP can be directly stored in the S3 data lake.

**Question 56**

**A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company’s VPCs must communicate with all other VPCs across all Regions.  
  
Which solution will meet these requirements with the LEAST amount of administrative effort?**

1. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications. Correct answer
2. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications
3. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
4. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.

**Overall explanation**

Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications:

* AWS Transit Gateway simplifies VPC connectivity, and peering Transit Gateways across Regions allows for centralized management of VPC communication across Regions.

**Question 57**

**A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.  
  
The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent.  
  
Which solution should a solutions architect recommend to meet these requirements?**

1. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.
2. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment. Correct answer
3. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
4. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

**Overall explanation**

Convert the application to use Amazon DynamoDB. Use a global table for the central reservation table. Use the correct Regional endpoint in each Regional deployment.

* Amazon DynamoDB global tables provide automatic multi-region replication, ensuring global consistency.

**Question 58**

**A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.  
  
Which solutions will meet these requirements? (Choose two.)**

1. Order an AWS Snowball Edge Storage Optimized device. Connect the device to the on-premises network. Copy data to the device by using the AWS CLI. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
2. Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system. Correct selection
3. Remove the drives from each file server. Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
4. Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
5. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

**Overall explanation**

Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.

* AWS DataSync can efficiently transfer data from on-premises servers to FSx for Windows File Server.

Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.

* This option involves using an AWS Snowcone device, a portable data transfer device. You would connect the Snowcone device to your on-premises network, launch DataSync agents on the device, and schedule DataSync tasks to transfer the data to FSx for Windows File Server. DataSync handles the migration process while preserving file permissions.

**Question 59**

**A company’s website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company’s website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.**

**Which combination should a solutions architect recommend to meet these requirements?**

1. Application Load Balancer with Amazon EC2 Auto Scaling
2. Amazon CloudFront and Amazon S3 Correct answer
3. AWS Lambda and Amazon DynamoDB
4. Amazon Route 53 with internal Application Load Balancers

**Overall explanation**

To meet the requirements of scaling globally, cost-effectiveness, minimal infrastructure provisioning, and fast response times for downloadable reports, you should recommend using Amazon CloudFront and Amazon S3.

Amazon CloudFront and Amazon S3

Amazon CloudFront is a content delivery network (CDN) service that provides low-latency and high-speed content delivery globally. You can use it to distribute your website's static content, including downloadable reports. Amazon S3 can store the reports, and CloudFront can cache and serve them from edge locations, reducing latency and providing a scalable and cost-effective solution.

This combination allows you to achieve fast response times, serve content globally, and reduce the load on your website's infrastructure.

**Question 60**

**A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.  
  
What is the MOST cost-effective solution?**

1. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).
2. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
3. Store the video archives in Amazon S3 Glacier and use Expedited retrievals. Correct answer
4. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

**Overall explanation**

By choosing Expedited retrievals in Amazon S3 Glacier, you can reduce the retrieval time to minutes, making it suitable for scenarios where quick access is required. Expedited retrievals come with a higher cost per retrieval compared to standard retrievals but provide faster access to your archived data.

**Question 61**

**A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.  
  
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)**

1. Use AWS Backup to take the backups and to keep the backups for 5 years. Correct selection
2. Configure an Amazon CloudWatch Logs export for the DB cluster.
3. Configure automated backup retention for 5 years.
4. Create a lifecycle policy for the automated backups.
5. Take a manual snapshot of the DB cluster.

**Overall explanation**

To meet the requirements of storing data in an Amazon Aurora PostgreSQL DB cluster for 5 years and retaining audit logs indefinitely, you should take the following steps:

1. Configure automated backup retention for 5 years:
   * Set up the automated backup retention period for the Aurora PostgreSQL DB cluster to 5 years.
2. Use Amazon CloudWatch Logs for audit logs:
   * Configure Amazon CloudWatch Logs export for the DB cluster to capture and store audit logs for an indefinite period.

These steps will ensure that your data is retained for 5 years, as required, while also capturing and retaining audit logs indefinitely. You do not need to create a manual snapshot or create a separate lifecycle policy for automated backups since you've already set up the automated backup retention period to meet the data retention requirement. AWS Backup is not typically used for the retention of database data, but rather for backing up a broader range of AWS resources.

**Question 62**

**A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.  
  
Which solution will meet these requirements MOST cost-effectively?**

1. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
2. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role. Correct answer
3. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
4. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.

**Overall explanation**

Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.

* AWS Lambda event source mapping with SQS FIFO queues ensures at-least-once processing for each request.
* Using AWS KMS for encryption provides security for the credit card data.
* Granting the kms:Decrypt permission allows the Lambda function to decrypt data when processing requests.

**Question 63**

**A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.  
  
How can a solutions architect ensure that the application has permission to access Amazon S3?**

1. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition. Correct answer
2. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.
3. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
4. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.

**Overall explanation**

Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.

Here's why:

1. Task Role: Amazon ECS allows you to specify an IAM role (task role) that can be assumed by the containers within your task. The task role is assumed by the containers, and they inherit the permissions associated with that role.
2. Least Privilege: It is recommended to follow the principle of least privilege, where you grant only the necessary permissions to the task. In your case, the task needs permissions to access Amazon S3, and you should create a custom IAM role with the required S3 permissions.
3. Task Definition: In your task definition, you can specify the taskRoleArn, which is the Amazon Resource Name (ARN) of the IAM role you created in step 2. By assigning this IAM role to your task, you are allowing your containers to access Amazon S3 with the permissions granted to that role.

This approach ensures that the application running in your Amazon ECS task has the required permissions to make Amazon S3 API calls while adhering to security best practices and following the principle of least privilege.

**Question 64**

**A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.  
  
Which storage option meets these requirements MOST cost-effectively?**

1. Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
2. Store the logs in Amazon CloudWatch Logs. Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
3. Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive. Correct answer
4. Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

**Overall explanation**

Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

Explanation:

To meet the requirements of retaining application log files for 10 years while optimizing cost, you can use Amazon S3 in combination with S3 Lifecycle policies. The application generates over 10 TB of logs per month, and older logs are rarely accessed.

Storing the logs in Amazon S3 for the most recent month (hot storage) ensures that the logs are readily available for troubleshooting, meeting the application team's needs. To minimize long-term storage costs, you can use S3 Lifecycle policies to automatically transition logs older than 1 month to a more cost-effective storage class, such as S3 Glacier Deep Archive.

S3 Lifecycle policies are a cost-effective way to manage data over time, moving it to different storage classes based on your specified criteria. In this case, moving logs older than 1 month to S3 Glacier Deep Archive helps minimize costs while retaining data for the required 10-year period.

**Question 65**

**A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.  
  
Which network design will meet these requirements?**

1. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.
2. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPUpdate the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses. Correct answer
3. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that references the security group ID of the application servers in eu-west-1.
4. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VPC. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.

**Overall explanation**

VPC Peering Connection:

This allows communication between instances in different VPCs as if they are on the same network. It's a straightforward approach to connect the two VPCs.

Subnet Route Tables:

After establishing the VPC peering connection, the subnet route tables need to be updated in both VPCs to route traffic to the other VPC's CIDR blocks through the peering connection. Inbound Rule in

Database Security Group:

By creating an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses, you ensure that only the specified application servers from the eu-west-1 VPC can access the database servers in the ap-southeast-2 VPC.

**Question 66**

**A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators.**

**Which solution will meet these requirements?**

1. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
2. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically. Correct answer
3. Configure the company’s email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
4. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

**Overall explanation**

To ensure that all future notifications are not missed and are limited to account administrators, you should use alternate contacts in AWS Organizations. This allows you to specify alternate contact email addresses for your AWS accounts, which are used for important notifications. Option B is the correct approach. Here's a more detailed explanation:

Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

With this approach:

1. You set up distribution lists (email groups) for the AWS account root user email addresses. This ensures that notifications are sent to multiple administrators, making it less likely that notifications are missed if the primary recipient is unavailable.
2. You configure AWS account alternate contacts in the AWS Organizations console or programmatically. Alternate contacts are separate email addresses where important AWS-related notifications, such as security and billing alerts, are sent. By specifying alternate contacts, you can ensure that specific individuals are responsible for monitoring and responding to alerts.
3. The alternate contacts will receive the notifications in addition to the root user's email address, which can also be a distribution list. This approach ensures redundancy and helps prevent missed notifications.
4. Using distribution lists for the root user email addresses allows for easier management of the recipients and ensures that the relevant administrators are included.

This approach helps you maintain visibility into notifications, involve multiple administrators in monitoring important alerts, and reduces the risk of missed notifications.

**Question 67**

**A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.  
  
The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.  
  
Which combination of steps will meet these requirements? (Choose three.)**

1. Use Amazon Comprehend to create the sentiment analysis reports. Correct selection
2. Use Amazon Lex to create the written sentiment analysis reports.
3. Use Amazon Transcribe to convert the audio recordings in any language into text. Correct selection
4. Use Amazon Comprehend to translate the audio recordings into English.
5. Use Amazon Translate to translate text in any language to English. Correct selection
6. Use Amazon Polly to convert the audio recordings into text.

**Overall explanation**

Use Amazon Transcribe to convert the audio recordings in any language into text.

Amazon Transcribe converts audio recordings into text, supporting multiple languages.

Use Amazon Translate to translate text in any language to English.

Amazon Translate is used to translate text to English, supporting multiple languages.

Use Amazon Comprehend to create the sentiment analysis reports.

Amazon Comprehend can analyze sentiment in the translated text, creating sentiment analysis reports.

**Question 68**

**A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital’s data team will scan the documents and will upload the documents to the AWS Cloud.  
  
A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.  
  
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)**

1. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
2. Write the document information to an Amazon EC2 instance that runs a MySQL database.
3. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text. Correct selection
4. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data. Correct selection
5. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.

**Question 69**

**A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.  
  
Which solution meets these requirements MOST cost-effectively?**

1. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity. Correct answer
2. Use Reserved Instances exclusively to handle the maximum capacity required.
3. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.
4. Use Spot Instances exclusively to handle the maximum capacity required.

**Overall explanation**

To meet the requirements of running an application on Amazon EC2 instances that processes messages from an Amazon SQS queue with unpredictable and intermittent traffic while ensuring continuous operation, the MOST cost-effective solution is:

Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.

Here's why this choice is appropriate:

* Reserved Instances (RIs) are ideal for providing a baseline capacity and offer cost savings compared to On-Demand instances. By reserving a portion of your expected capacity using RIs, you can ensure that a certain number of instances are always available.
* Spot Instances are the most cost-effective option for handling variable or additional capacity. Since the message volume is unpredictable, you can take advantage of Spot Instances when available to scale your application horizontally during peak traffic without incurring high costs. Spot Instances are available at significantly lower prices than On-Demand instances, making them cost-effective for bursty workloads.

This combination of RIs for the baseline capacity and Spot Instances for handling fluctuations in traffic allows for cost savings while ensuring continuous operation and scalability when needed. It is a cost-effective and efficient way to manage the workload while keeping costs in check.

**Question 70**

**A company has a data ingestion workflow that includes the following components:  
An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries  
An AWS Lambda function that processes and stores the data  
The ingestion workflow occasionally fails because of network connectivity issues. When failure occurs, the corresponding data is not ingested unless the company manually reruns the job.  
  
What should a solutions architect do to ensure that all notifications are eventually processed?**

1. Configure the SNS topic’s retry strategy to increase both the number of retries and the wait time between retries.
2. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue. Correct answer
3. Configure the Lambda function for deployment across multiple Availability Zones.
4. Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.

**Overall explanation**

Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue.

Explanation:

To ensure that all notifications are eventually processed and to handle intermittent failures in the data ingestion workflow, it's a best practice to introduce a queue mechanism. Configuring an Amazon SQS queue as the on-failure destination for the Amazon SNS topic and modifying the Lambda function to process messages from the queue allows for better fault tolerance and reliable message processing. If a network connectivity issue or any other transient failure occurs during the data ingestion process, the notification message is placed in the SQS queue, ensuring that it's not lost, and the Lambda function can process it when connectivity is restored or the issue is resolved.

Amazon SQS provides message queuing for decoupling the sender of a message from its receiver, which is ideal for addressing reliability and fault tolerance issues in workflows like this. It helps ensure that notifications are eventually processed, even in cases of transient failures or issues.

**Question 71**

**A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.  
  
Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Choose two.)**

1. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance. Correct selection
2. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance
3. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.
4. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website
5. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website. Correct selection

**Overall explanation**

Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.

* Amazon EFS provides scalable and shared file storage that can be mounted on multiple EC2 instances.

Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.

* The Auto Scaling group maintains a minimum of two instances, ensuring resilience by automatically replacing any unhealthy instances. Additionally, configuring an Amazon CloudFront distribution for the website further improves performance by caching content at edge locations closer to the end-users, reducing latency and improving content delivery.

**Question 72**

**A company has an AWS account used for software engineering. The AWS account has access to the company’s on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.  
  
A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company’s data center.  
  
Which solution will meet these requirements?**

1. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
2. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.
3. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
4. Configure the Lambda function to run in the VPC with the appropriate security group. Correct answer

**Overall explanation**

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

When you configure an AWS Lambda function to run within a Virtual Private Cloud (VPC), you are essentially providing the Lambda function with the ability to access resources within that VPC. In the context of your scenario, where you need the Lambda function to access a database that resides in a private subnet of your on-premises data center, running the Lambda function within a VPC is a critical part of the solution.

Here's how it works:

1. Running Lambda in a VPC: When you configure the Lambda function to run within a VPC, it gets associated with a specific VPC. This means the Lambda function operates within the network boundaries of the VPC.
2. Access to Private Subnets: If your on-premises data center is connected to this VPC through Direct Connect or VPN, the Lambda function can access resources in your VPC, including those in the private subnets.
3. Security Group: By specifying an appropriate security group, you can control the inbound and outbound network traffic to and from the Lambda function. In your case, you would configure the security group to allow outbound connections to your database server in the private subnet.

By configuring the Lambda function to run in the VPC with the correct security group rules, you ensure that it can securely communicate with the database in your on-premises data center.

This approach provides isolation, security, and controlled network access, making it possible for the Lambda function to interact with on-premises resources while benefiting from AWS's scalability and serverless computing capabilities.

**Question 73**

**A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zone:  
  
What should a solutions architect do to meet this requirement?**

1. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.
2. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
3. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance. Correct answer
4. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.

**Overall explanation**

Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.

Here's why:

* Amazon FSx for Windows File Server is a fully managed Windows file system that is accessible from multiple Amazon EC2 instances and is built to natively support Windows applications. It's designed for scenarios where you need a shared file system across multiple Windows instances, and it can be accessed simultaneously from multiple instances in different Availability Zones.
* Amazon Elastic File System (Amazon EFS) can also provide shared file storage, but it is more suited for Linux instances and doesn't natively support Windows file system semantics.
* Amazon Elastic Block Store (Amazon EBS) volumes can be attached to a single EC2 instance at a time and do not inherently support simultaneous access from multiple instances.
* AWS Storage Gateway in volume gateway mode provides block-level access to data and might not be the best fit for a shared file system requirement.

So, for a Windows-based application that needs a shared Windows file system attached to multiple EC2 Windows instances across multiple Availability Zones, Amazon FSx for Windows File Server is the most suitable choice.

**Question 74**

**A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application’s traffic recently spiked due to fraudulent requests from botnets.  
  
Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)**

1. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
2. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses. Correct selection
3. Create a usage plan with an API key that is shared with genuine users only.
4. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out. Correct selection
5. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

**Overall explanation**

To block requests from unauthorized users and protect the serverless application, you should take the following steps:

Implement an AWS WAF (Web Application Firewall) rule to target malicious requests and trigger actions to filter them out. AWS WAF allows you to filter traffic at the web application layer and provides protection against common web exploits and security threats.

Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses. In addition to AWS WAF, you can also implement custom logic within your Lambda function to block or ignore requests from known fraudulent IP addresses.

**Question 75**

**A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.  
  
Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)**

1. Deploy an AWS Storage Gateway file gateway to replace NFS storage. Correct selection
2. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers. Correct selection
3. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
4. Mount Amazon S3 as a file system to the on-premises servers.
5. Deploy an AWS Storage Gateway volume gateway to replace the block storage.

**Overall explanation**

1. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
   * AWS Storage Gateway file gateway provides a scalable and cost-effective solution for file storage.
2. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.
   * Amazon EFS volumes can be mounted on-premises and provide a scalable file system.

**Question 76**

**A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.  
Which solution will meet these requirements?**

1. Use AWS DataSync to connect the S3 buckets to the web application.
2. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
3. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers. Correct answer
4. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

**Overall explanation**

To meet the requirement of delivering content quickly to users around the world and ensuring reliable access to confidential media files stored in Amazon S3 buckets, the best solution is to deploy Amazon CloudFront. So, the correct answer is:

Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.

Here's why this is the most suitable option:

1. Amazon CloudFront is a content delivery service that uses a global network of edge locations to cache and serve content to users from the nearest edge location. This results in lower latency and faster content delivery to users worldwide.
2. By deploying Amazon CloudFront, you can ensure that the confidential media files are cached at edge locations, reducing the load on the S3 buckets and providing faster access to the content for users, regardless of their geographic location.
3. AWS Global Accelerator is used for improving availability and application fault tolerance, but it doesn't directly address content caching.
4. AWS DataSync is used for data transfer and synchronization, which may not provide the caching and content delivery benefits needed for this use case.
5. Amazon Simple Queue Service (Amazon SQS) is a message queuing service and isn't designed for content caching and delivery.

Amazon CloudFront is the AWS service designed for delivering content with low latency and high availability, making it the most appropriate choice for this scenario.

**Question 77**

**A company runs an Oracle database on premises. As part of the company’s migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.**

**Which solution will meet these requirements?**

1. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.
2. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
3. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region. Correct answer
4. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.

**Overall explanation**

Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.

This Option involves migrating the Oracle database to Amazon RDS for Oracle, which is a managed database service that reduces operational overhead. This choice also includes creating a read replica for the database in another AWS Region, which serves as the disaster recovery (DR) solution. Here's why this option is valid:

1. Amazon RDS for Oracle: Using Amazon RDS for Oracle simplifies database management tasks, such as backups, software patching, and maintenance. This significantly reduces operational overhead, making it a suitable choice for the company's needs.
2. Read Replica in Another AWS Region: By creating a read replica in a different AWS Region, you achieve geographic redundancy and a form of disaster recovery. If the primary database in one Region becomes unavailable due to a Region-level issue, you can promote the read replica in the secondary Region to the primary database.

This approach provides high availability, and disaster recovery, and minimizes operational management while allowing the company to use Amazon RDS for Oracle, a fully managed service.

**Question 78**

**A company is making a prototype of the infrastructure for its new website by manually provisioning the necessary infrastructure. This infrastructure includes an Auto Scaling group, an Application Load Balancer and an Amazon RDS database. After the configuration has been thoroughly validated, the company wants the capability to immediately deploy the infrastructure for development and production use in two Availability Zones in an automated fashion.  
  
What should a solutions architect recommend to meet these requirements?**

1. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones
2. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.
3. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones.
4. Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation. Correct answer

**Overall explanation**

Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation:

* AWS CloudFormation provides infrastructure as code (IaC) capabilities, allowing you to define and provision AWS infrastructure in an automated and repeatable manner.
* By defining the infrastructure as a CloudFormation template, you can easily deploy it to different environments, such as development and production, in two Availability Zones.

**Question 79**

**A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company’s HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.  
  
The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.  
  
Which combination of AWS services meets these requirements?**

1. Amazon FSx for Lustre integrated with Amazon S3 Correct answer
2. Amazon FSx for Windows File Server integrated with Amazon S3
3. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume
4. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)

**Overall explanation**

To meet the company's requirements for high performance computing (HPC) with data copying from on-premises, data integration with persistent storage, and high-performance file system, option A, "Amazon FSx for Lustre integrated with Amazon S3," is the most appropriate choice. Here's why:

1. Amazon FSx for Lustre: This service is designed for high-performance file storage. It is well-suited for HPC workloads and can provide high throughput, low latency, and scalability. It can be easily integrated with EC2 instances to provide a shared file system for your HPC workloads.
2. Amazon S3: You can copy on-premises data to Amazon S3 for long-term storage. Amazon S3 is a scalable and durable object storage service that can serve as the data lake for your organization, and it integrates well with other AWS services.

This option allows you to use Amazon FSx for Lustre for your HPC file system needs while leveraging Amazon S3 for data storage, ensuring high performance and integration with persistent storage for analytics and future use.

**Question 80**

**An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that some of the order messages were not received.  
  
A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.  
  
Which solution will meet these requirements with the LEAST development effort?**

1. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.
2. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days. Correct answer
3. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
4. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.

**Overall explanation**

Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days:

* This setup utilizes the dead letter queue of Amazon SNS with an SQS target to retain and analyze messages for up to 14 days.

**Question 81**

**A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.  
  
Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)**

1. Set up an Amazon Cognito identity pool. Configure AWS IAM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.
2. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.
3. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization. Correct selection
4. Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service. Correct selection
5. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service.

**Overall explanation**

Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.

This is the initial step to create a new organization and AWS accounts.

Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center and integrate it with the company's corporate directory service.

AWS IAM Identity Center (AWS SSO) provides centralized authentication for AWS accounts.

Integrating it with the corporate directory service ensures centralized authentication.

**Question 82Skipped**

**A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight. Application usage is low during weekends.  
The company wants to minimize its EC2 costs without affecting the availability of the application.  
  
Which solution will meet these requirements?**

1. Use Spot Instances for the entire workload.
2. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.
3. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
4. Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs. Correct answer

**Overall explanation**

Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs.

Explanation:

In this scenario, the company wants to minimize EC2 costs without affecting the availability of the application. The application experiences different levels of usage during the day, with heavy usage during business hours and lower usage during the evening and weekends.

Using Reserved Instances for the baseline level of usage is a cost-effective approach. Reserved Instances provide significant cost savings when you have a predictable and consistent workload, which is the case during the baseline hours.

However, during peak usage periods when additional capacity is required, using Spot Instances (which are typically lower in cost) for the extra capacity is a practical solution. This allows the company to maintain availability during high-demand times while keeping costs down.

This hybrid approach combines the cost savings of Reserved Instances with the flexibility and lower costs of Spot Instances, ensuring that the company can efficiently manage its EC2 costs while meeting application demand.

**Question 83**

**A law firm needs to share information with the public. The information includes hundreds of files that must be publicly readable. Modifications or deletions of the files by anyone before a designated future date are prohibited.  
  
Which solution will meet these requirements in the MOST secure way?**

1. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects. Correct answer
2. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
3. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.
4. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.

**Overall explanation**

Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects:

* S3 Object Lock helps enforce retention policies and prevents modifications or deletions during the retention period.
* Using S3 Versioning ensures a versioned history of objects, and configuring static website hosting allows for public readability.

**Question 84**

**A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts.  
  
Which solution will meet these requirements?**

1. Attach an identity-based policy to deny access to the billing information to all users, including the root user.
2. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.
3. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.
4. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU). Correct answer

**Overall explanation**

Create a service control policy (SCP) to deny access to the billing information. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service:

* SCPs can restrict access across the AWS Organization.
* Adding AWS SSO to AWS Directory Service ensures centralized authentication.

**Question 85**

**A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.  
  
Which service will improve the performance of both the real-time and on-demand streaming?**

1. Amazon S3 Transfer Acceleration
2. Amazon CloudFront Correct answer
3. Amazon Route 53
4. AWS Global Accelerator

**Overall explanation**

To improve the performance of both real-time and on-demand streaming for a global online audience, Amazon CloudFront is the ideal service. Amazon CloudFront is a content delivery network (CDN) service that can accelerate the delivery of web content, including videos and streaming content, to users across the globe by caching content at edge locations.

**Question 86**

**A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job’s runtime varies between 1 minute and 3 minutes.  
  
Which solution will meet these requirements MOST cost-effectively?**

1. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes. Correct answer
2. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every  
   10 minutes.
3. Create an AWS Lambda function based on the container image of the job. Configure Amazon EventBridge to invoke the function every 10 minutes.
4. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.

**Overall explanation**

Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes:

* Running the job on Amazon ECS with Fargate allows for serverless container execution.
* Creating a scheduled task ensures that the job runs every 10 minutes, meeting the specified requirement.
* This is a cost-effective solution as Fargate eliminates the need to manage underlying infrastructure.

**Question 87**

**A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly.  
  
Which solution will meet these requirements MOST cost-effectively?**

1. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
2. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.
3. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group. Correct answer
4. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.

**Overall explanation**

Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template. Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

Explanation:

The requirement is to make the application scale seamlessly and cost-effectively during busy times. Here's why this option is the best choice:

1. Database Migration: Migrating the database to Amazon Aurora MySQL is a good choice because Aurora is a highly available and scalable database service that can handle the increased load more efficiently than hosting the database on a single EC2 instance.
2. AMI and Launch Template: Creating an Amazon Machine Image (AMI) of the web application and using a launch template allows you to easily replicate the web application on additional instances when needed.
3. Auto Scaling: By using an Auto Scaling group with a Spot Fleet, you can automatically launch new instances when the load increases. Spot instances are a cost-effective choice and can save money compared to On-Demand instances.
4. Application Load Balancer: Attaching an Application Load Balancer to the Auto Scaling group allows you to distribute traffic evenly across the EC2 instances, ensuring high availability and seamless scaling.

This solution not only improves application performance but also optimizes cost by leveraging Amazon Aurora, Auto Scaling, and Spot Fleet for efficient resource management.

**Question 88**

**A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts. The company wants to centrally restrict the creation of AWS resources in these accounts.  
  
Which solution will meet these requirements with the LEAST development effort?**

1. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types.
2. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances.
3. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types. Ensure that staff can deploy EC2 instances only by using the Service Catalog products.
4. Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types. Correct answer

**Overall explanation**

Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.

* AWS Organizations allows central management of accounts.
* Service Control Policies (SCPs) provide fine-grained control over AWS services and actions.
* Defining an SCP at the organizational unit level restricts the usage of EC2 instance types centrally.

**Question 89**

**A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table.  
  
Which solution meets these requirements?**

1. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table. Correct answer
2. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.
3. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.
4. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.

**Overall explanation**

Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table:

* DynamoDB continuous backups allow point-in-time recovery without affecting availability or read capacity units (RCUs).
* Direct export to Amazon S3 ensures minimal coding effort and meets the specified requirements.

**Question 90**

**A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.  
  
Which solution meets these requirements with the MOST scalability?**

1. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.
2. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket. Correct answer
3. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.
4. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

**Overall explanation**

Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.

* Using presigned URLs allows users to upload files directly to S3, providing a scalable and efficient solution.

**Question 91**

**A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.  
  
The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.  
  
Which solution meets these requirements MOST cost-effectively?**

1. Deploy an Amazon CloudFront web distribution in front of the S3 bucket. Correct answer
2. Deploy an AWS Global Accelerator accelerator in front of the web servers.
3. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.
4. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.

**Overall explanation**

Deploy an Amazon CloudFront web distribution in front of the S3 bucket.

Explanation:

Amazon CloudFront is a content delivery network (CDN) service that caches and distributes content globally. It is designed to serve content to end-users with low latency and high data transfer speeds. When it comes to serving static media files like videos and images stored in Amazon S3 to a large number of users worldwide, CloudFront is an excellent choice. Here's why it's the right choice:

1. Global Content Distribution: CloudFront has a global network of edge locations, so it can cache content close to the users, reducing latency and load on the origin server.
2. Cost-Efficiency: CloudFront is cost-effective because it caches content at the edge, reducing the need to retrieve content from the origin repeatedly.
3. Scalability: CloudFront scales automatically to handle traffic spikes, ensuring a smooth user experience, even during popularity surges.
4. Origin Shield: You can configure an additional caching layer called an "origin shield" for added load reduction on the S3 bucket. It acts as an intermediate cache between the edge locations and the S3 bucket, reducing the number of requests reaching the origin.
5. Security: You can configure security features in CloudFront to restrict access and protect your content.

Deploying CloudFront in front of your S3 bucket is the most cost-effective and efficient way to serve your media files to a global audience while reducing the load on the origin server.

**Question 92**

**A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target m each Availability Zone within a Region.  
  
A solutions architect wants to use AWS Backup to manage the replication to another Region.  
  
Which solution will meet these requirements?**

1. Amazon FSx for Windows File Server with a Multi-AZ deployment
2. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment
3. Amazon FSx for OpenZFS
4. Amazon Elastic File System (Amazon EFS) with the Standard storage class

**Overall explanation**

EFS Replication can replicate your file system data to another Region or within the same Region without requiring additional infrastructure or a custom process. Amazon EFS Replication automatically and transparently replicates your data to a second file system in a Region or AZ of your choice. You can use the Amazon EFS console, AWS CLI, and APIs to activate replication on an existing file system. EFS Replication is continual and provides a recovery point objective (RPO) and a recovery time objective (RTO) of minutes, helping you meet your compliance and business continuity goals.

**Question 93**

**A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of reads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.  
  
What should the solutions architect do to meet this requirement?**

1. Add Amazon RDS read replicas. Correct answer
2. Use Amazon ElastiCache for Memcached.
3. Use Amazon ElastiCache for Redis.
4. Use Amazon Route 53 DNS caching

**Overall explanation**

Add Amazon RDS read replicas.

To reduce the number of database reads while ensuring high availability, you can add Amazon RDS read replicas. Amazon RDS read replicas can offload read traffic from the primary RDS instance, thus reducing the load on the primary database. This can help improve the performance of your batch application and ensure that high availability is maintained because read replicas are read-only copies that can be used for scaling out read workloads and for failover in case of primary database issues.

**Question 94**

**A company is building a containerized application on premises and decides to move the application to AWS. The application will have thousands of users soon after it is deployed. The company is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.  
  
Which solution will meet these requirements?**

1. Store container images in a repository that runs on an Amazon EC2 instance. Run the containers on EC2 instances that are spread across multiple Availability Zones. Monitor the average CPU utilization in Amazon CloudWatch. Launch new EC2 instances as needed.
2. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers. Use target tracking to scale automatically based on demand.
3. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand. Correct answer
4. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image. Launch EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.

**Overall explanation**

For a highly available architecture that minimizes operational overhead, option A, which uses AWS Fargate with automatic scaling, is the most suitable choice. Here's why:

Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand.

With this option:

1. AWS Fargate: AWS Fargate is a serverless compute engine for containers. It abstracts infrastructure management and allows you to focus on running containers without managing the underlying instances. Fargate handles the scaling, patching, and updates, minimizing operational overhead.
2. Amazon ECR: Storing container images in Amazon ECR ensures a secure and reliable repository for your images.
3. Target Tracking Scaling: Using target tracking in ECS allows you to automatically scale the number of tasks (containers) based on defined target metrics. It helps ensure that the application can handle increased demand without manual intervention.

**Question 95**

**A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.  
  
What should a solutions architect do to meet these requirements?**

1. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.
2. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
3. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
4. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group. Correct answer

**Overall explanation**

Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Here's an explanation for this choice:

* AWS Global Accelerator is a service that uses anycast IP addresses to route traffic to the nearest edge location based on health, geography, routing policies, and more. It's ideal for improving the availability, performance, and resilience of applications, especially for gaming where latency is critical.
* Using a Network Load Balancer (NLB) can provide efficient load balancing for UDP-based traffic as NLB supports the UDP protocol.
* Amazon EC2 instances in an Auto Scaling group provide the compute resources necessary for your gaming application, and they can scale based on demand.

This configuration allows the front-end tier to efficiently route traffic to the nearest edge location using AWS Global Accelerator while providing a highly available and scalable backend using a Network Load Balancer and EC2 Auto Scaling. It also ensures static IP addresses are available to your users for entry into the application endpoints, providing a seamless and performant gaming experience.

**Question 96Skipped**

**A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.  
  
Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)**

1. Create an ongoing replication task. Correct selection
2. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
3. Create a database backup of the on-premises database.
4. Create an AWS Database Migration Service (AWS DMS) replication server. Correct selection
5. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

**Overall explanation**

To migrate an on-premises PostgreSQL database to Amazon Aurora PostgreSQL while keeping the on-premises database online and ensuring synchronization, you should perform the following steps:  
  
Create an ongoing replication task using AWS Database Migration Service (AWS DMS): This replication task will continuously capture changes from the source database (on-premises PostgreSQL) and apply them to the target database (Amazon Aurora PostgreSQL). This keeps both databases in sync during and after the migration.

Create an AWS Database Migration Service (AWS DMS) replication server: The replication server is used to manage replication tasks, and it's an essential component for ongoing data replication.

**Question 97**

**A company is building a three-tier application on AWS. The presentation tier will serve a static website The logic tier is a containerized application. This application will store data in a relational database. The company wants to simplify deployment and to reduce operational costs.  
  
Which solution will meet these requirements?**

1. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database. Correct answer
2. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
3. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
4. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

**Overall explanation**

Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.

Hosting static content in Amazon S3, using ECS with Fargate for compute, and a managed RDS cluster simplifies deployment and reduces operational costs.

**Question 98**

**A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company’s security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company’s VPC.  
  
Which solution will mast these requirements?**

1. Create a NAT gateway in a public subnet of the company’s VPUpdate the route table to connect to the target service.
2. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
3. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.
4. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service. Correct answer

**Overall explanation**

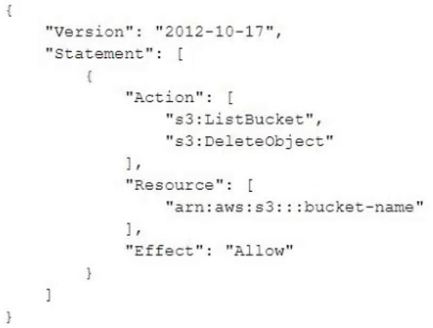
Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

Here's why this is the best option:

* VPC Endpoint: A VPC endpoint allows private, direct communication to AWS services (or services hosted in other VPCs) without traversing the public internet. It ensures that connectivity to the external provider's service remains private.
* AWS PrivateLink: AWS PrivateLink is used to access services over an Amazon network rather than the public internet. It provides a secure and efficient way to access services like the external provider's service.

This approach ensures that the connection is initiated only from the company's VPC, and it is both private and secure.

**Question 99**

**A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.  
  
**

**Which statement should a solutions architect add to the policy to correct bucket access?**

1. **"Action": ["s3: DeleteObject"],  
   "Resource": ["arn:aws:s3:::bucket-name/\*"],  
   "Effect":"Allow" Correct answer**
2. **"Action": ["s3: \*"],  
   "Resource": ["arn:aws:s3:::bucket-name/\*"],  
   "Effect":"Allow"**
3. **"Action": ["s3: DeleteObject"],  
   "Resource": ["arn:aws:s3:::bucket-name\*"],  
   "Effect":"Allow"**
4. **"Action": ["s3: \*Object"],  
   "Resource": ["arn:aws:s3:::bucket-name/\*"],  
   "Effect":"Allow"**

**Overall explanation**

Action is S3:\*. this means all actions. The company follows least-privilege access rules.

**Question 100**

**A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.  
  
Which combination of solutions provides the MOST protection? (Choose two.)**

1. Use Amazon GuardDuty with AWS Shield Standard
2. Use AWS Shield Standard with Amazon API Gateway.
3. Use AWS WAF to protect Amazon API Gateway. Correct selection
4. Use AWS WAF to protect the NLB.
5. Use AWS Shield Advanced with the NLB. Correct selection

**Overall explanation**

To provide the MOST protection for the cloud communications platform, you should use the following combination of solutions:

1. Use AWS WAF to protect Amazon API Gateway: AWS Web Application Firewall (WAF) is a service that helps protect web applications from common web exploits, such as SQL injection. You can configure AWS WAF to inspect and filter incoming API requests for malicious content, providing a layer of protection for your APIs hosted on Amazon API Gateway.
2. Use AWS Shield Advanced with the Network Load Balancer (NLB): AWS Shield Advanced is a managed Distributed Denial of Service (DDoS) protection service that offers enhanced protection against large and sophisticated DDoS attacks. By configuring AWS Shield Advanced with your Network Load Balancer (NLB), you can mitigate DDoS attacks at the network level, ensuring high availability and uptime for your application.

This combination of AWS WAF for API security and AWS Shield Advanced for DDoS protection helps to safeguard your cloud communications platform against both web exploits and large-scale attacks. It provides comprehensive security for your application.

**Question 101**

**A company runs its ecommerce application on AWS. Every new order is published as a massage in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone.  
The company needs to redesign its architecture to provide the highest availability with the least operational overhead.  
  
What should a solutions architect do to meet these requirements?**

1. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database
2. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
3. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
4. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL. Correct answer

**Overall explanation**

To provide the highest availability with the least operational overhead, you should choose a solution that includes a highly available queue service, an auto-scaling group for the application, and a managed database service. The best option in this scenario is:

Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.

Here's an explanation for this choice:

1. Migrating the queue to Amazon MQ with a redundant pair of RabbitMQ instances provides a highly available message broker with active/standby architecture.
2. Creating a Multi-AZ Auto Scaling group for EC2 instances hosting the application ensures that the application can scale and provides high availability in case of EC2 instance failures within multiple Availability Zones.
3. Migrating the database to Amazon RDS for PostgreSQL with a Multi-AZ deployment ensures that the database is highly available and provides automated failover in case of database instance failures.

This architecture minimizes operational overhead because it leverages managed services (Amazon MQ and Amazon RDS) for the message queue and database. It also offers high availability and fault tolerance across multiple Availability Zones, helping to ensure that your application remains resilient even in the event of infrastructure failures.

**Question 102**

**A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.  
  
The administrator is using an IAM role that has the following IAM policy attached:**

****

**What is the cause of the unsuccessful request?**

1. The EC2 instance has a resource-based policy with a Deny statement.
2. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24. Correct answer
3. The "Action" field does not grant the actions that are required to terminate the EC2 instance.
4. The principal has not been specified in the policy statement.

**Overall explanation**

" aws:SourceIP " indicates the IP address that is trying to perform the action.

**Question 103**

**A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.  
  
Which solution will meet these requirements?**

1. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon Aurora with Aurora Auto Scaling for the database.
2. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon DynamoDB with provisioned write capacity for the database.
3. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon Aurora with Aurora Auto Scaling for the database. Configure Amazon CloudFront to deliver the website content.
4. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content. Correct answer

**Overall explanation**

Host static content in Amazon S3. Host dynamic content using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content.

Here's why:

1. Static content in Amazon S3: Hosting static content in S3 is cost-effective, highly available, and requires minimal maintenance. S3 can handle website assets like images, CSS, and JavaScript.
2. Dynamic content with API Gateway and Lambda: API Gateway and Lambda allow you to build a serverless backend for your dynamic content, eliminating the need to manage servers. It can scale automatically based on demand and provide high availability.
3. Amazon DynamoDB with on-demand capacity: Using on-demand capacity for DynamoDB means you don't have to provision read and write capacity in advance. It will automatically scale based on the actual usage, ensuring high availability and minimal management overhead.
4. Amazon CloudFront: CloudFront helps deliver the website content globally with low latency and high availability.

**Question 104**

**A company is conducting an internal audit. The company wants to ensure that the data in an Amazon S3 bucket that is associated with the company’s AWS Lake Formation data lake does not contain sensitive customer or employee data. The company wants to discover personally identifiable information (PII) or financial information, including passport numbers and credit card numbers.  
  
Which solution will meet these requirements?**

1. Use Amazon S3 Select to run a report across the S3 bucket.
2. Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types. Correct answer
3. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.
4. Configure Amazon S3 Inventory on the S3 bucket Configure Amazon Athena to query the inventory.

**Overall explanation**

Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.

* Amazon Macie can identify personally identifiable information (PII) and financial information using managed identifiers.

**Question 105**

**A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company’s security policy requires that all website traffic be inspected by AWS WAF.  
  
How should the solutions architect comply with these requirements?**

1. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
2. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
3. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
4. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution. Correct answer

**Overall explanation**

Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Here's why this option is correct:

1. Origin Access Identity (OAI): Using an OAI with CloudFront is a best practice for securing access to your S3 origin. It allows you to restrict direct access to your S3 bucket, ensuring that all requests go through CloudFront.
2. AWS WAF: Enabling AWS WAF on the CloudFront distribution ensures that all incoming traffic is inspected by the Web Application Firewall, allowing you to filter and protect against web application threats.

This combination of OAI for S3 and AWS WAF for CloudFront helps secure your static website and ensures that all traffic is inspected as required by the security policy.