Question1 : A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.
Which solution meets these requirements?

A: Enable Amazon GuardDuty on the account.

B: Enable Amazon Inspector on the EC2 instances.

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

D: Enable AWS Shield Advanced and assign the ELB to it.

Explanation : Explanation :AWS Shield Advanced provides cost-effective protection for larger and more complex attacks. It can protect your AWS applications deployed on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and more against DDoS attacks.

Answer: D

Question2 : A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.
The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.
What is the MOST operationally efficient solution that meets these requirements?

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

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

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

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

Explanation : Explanation :Amazon Kinesis Data Firehose is built to automatically scale to match the throughput of your data and requires no ongoing administration. It can capture, transform, and load data streams into AWS data stores. Amazon S3 provides simple storage service, you can transition to S3 Glacier for cost-effective long-term storage after 14 days as per the requirement.

Answer: A

Question3 : A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.
What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

A: Launch the NAT gateway in each Availability Zone.

B: Replace the NAT gateway with a NAT instance.

C: Deploy a gateway VPC endpoint for Amazon S3.

D: Provision an EC2 Dedicated Host to run the EC2 instances.

Explanation : Explanation :Deploying a gateway VPC endpoint for Amazon S3 will allow the EC2 instances to directly access S3 without going through a NAT gateway, thus avoiding data transfer charges.

Answer: C

Question4 : A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.
Which solution meets these requirements?

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

B: Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.

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

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

Explanation : Explanation :AWS Direct Connect is a network service that provides an alternative to using the Internet to utilize AWS cloud services. By establishing a dedicated network connection from the on-premises network to AWS, we can bypass internet service providers in the network path which increases bandwidth throughput and provides a more consistent network experience when accessing AWS cloud services. Therefore, it allows for timely backups to S3 without impacting the internet connectivity for internal users.

Answer: B

Question5 : A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.
Which combination of configuration options will meet these requirements? (Choose two.)

A: Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS

Multi-AZ DB instance in private subnets.

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

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

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

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

Explanation : Explanation :Option A is chosen because launching EC2 instances in private subnets ensures that they are not exposed to the internet. Using an Auto Scaling group enhances availability. An RDS Multi-AZ DB instance enhances high availability and fault tolerance. Option B is chosen because configuring a VPC with private subnets and NAT gateways ensure that the EC2 instances have internet access for payment processing without being exposed to the public internet. Deploying an Application Load Balancer in the private subnets helps distribute incoming traffic.

Answer: AB

Question6 : A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.
A solutions architect needs to minimize the time that is required to clone the production data into the test environment.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :Option D would allow for the quickest restoration of data from the EBS snapshot to the test environment by leveraging the EBS Fast Snapshot Restore (FSR) feature. This feature allows the snapshots to initialize instantaneously to their full performance capacity, thus reducing the time required to clone the production data into the test environment. Also, by creating new EBS volumes for the test environment, it ensures that the modifications to the cloned data do not affect the production environment.

Answer: D

Question7 : A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege. Which solution will meet these requirements?

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

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

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

D: Deploy a bastion server in a public subnet. When the product manager requires access to the

dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Explanation : Explanation :The option B is the most appropriate solution as it strictly adheres to the 'principle of least privilege'. Creating an IAM user specifically for the product manager and assigning them the CloudWatchReadOnlyAccess simply gives them read-only access to CloudWatch which is enough for them to view the dashboard. This way, the product manager has the least necessary privileges needed for them to perform their job. The other options either provide excess permissions, are complicated, or depend on manual actions like searching for the dashboard.

Answer: B

Question8 : A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :Option A will meet the requirements. Because the company is already using AWS Organizations and needs a single sign-on (SSO) solution, AWS Single Sign-On (AWS SSO) is the best choice. Enabling AWS SSO and establishing a one-way trust with the Microsoft Active Directory allows the company to continue managing its users and groups on-premises.

Answer: A

Question9 : A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.
Which solution meets these requirements MOST cost-effectively?

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

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

C: Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.

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

Explanation : Explanation :Adding an Amazon CloudFront distribution in front of the S3 bucket and editing the Route 53 entries to point to the CloudFront distribution will most cost-effectively meet the requirements. CloudFront is designed to optimize the performance of content delivery to users by ensuring it is served from the location that provides the lowest latency. Hence, this minimizes latency for users who access the website.

Answer: C

Question10 : A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.
Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.
What should a solutions architect do to meet these requirements with the LEAST development effort?

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

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

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

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

Explanation : Explanation :Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data including PII. Amazon Simple Notification Service (Amazon SNS) would trigger a notification to the administrators as soon as it detects the PII, which would allow the administrators to take immediate actions to remove the PII. This method would handle the situation with the least amount of development effort.

Answer: B

Question11 : A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically. is highly available, and requires minimum operational overhead.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :Amazon EC2 instances in a Multi-AZ Auto Scaling group is suitable for scalability and high availability. Also, Amazon Elastic File System (Amazon EFS) is designed to store large amounts of data in a standard file system structure, which fulfills the company's needs better than the other options.

Answer: C

Question12 : A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :The solution that will meet these requirements is the creation of a regional API Gateway endpoint. The company needs to associate the API Gateway endpoint with its domain name, import the public certificate associated with its domain name into AWS Certificate Manager (ACM) in the same region, as well as attach the certificate to the API Gateway endpoint. Then, they need to configure Route 53 to route traffic to the API Gateway endpoint. This way the company's domain name and certificate are used securely in the public interface for its backend microservice APIs.

Answer: C

Question13 : A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days. Which storage solution is MOST cost-effective?

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

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

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

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

Explanation : Explanation :Choosing this option because it is the most cost-effective solution, and remains immediate accessible which is required by the business. S3 Standard-IA is designed for larger data where data is accessed less frequently, but it still needs the quick access when needed, such as in this case scenario where files are rarely accessed after first 30 days.

Answer: C

Question14 : A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.
A solutions architect needs to design a solution that stores customer data that is created during database upgrades.
Which solution will meet these requirements?

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

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

C: Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.

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

Explanation : Explanation :Storing the customer data in an Amazon Simple Queue Service (SQS) FIFO queue would ensure that the data is not lost and can be processed once the upgrade is complete. Creating a new Lambda function that polls the queue and stores the customer data in the database after the upgrade ensures no data loss during the upgrade.

Answer: D

Question15 : A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours.
The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.
Which solution will meet this requirement with the LEAST operational overhead?

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

B: Create a read replica of the database. Configure the script to query only the read replica.

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

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

Explanation : Explanation :Creating a read replica of the database would offload the read traffic from the main instance, thus improving performance. The script can then be adjusted to query only the read replica, effectively segregating the write and read operations and improving overall performance.

Answer: B

Question16 : A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.
Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)

A: Use AWS Shield Advanced to stop the DDoS attack.

B: Configure Amazon GuardDuty to automatically block the attackers.

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

D: Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.

E: Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.

Explanation : Explanation :AWS Shield Advanced is specifically designed to help protect an application against DDoS attacks. Amazon CloudFront is used to deliver both static and dynamic website content, and it can use AWS Shield for DDoS protection making it effective against such

attacks. While options B, D, and E might provide certain benefits in a broader security context, they are not specifically geared toward mitigating a large-scale DDoS attack.

Answer: AC

Question17 : A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.
How should security groups be configured in this situation? (Choose two.)

A: Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.

B: Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.

C: Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.

D: Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.

E: Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Explanation : Explanation :Option A ensures that incoming traffic from the internet can reach the public-facing web tier, which is necessary for the operation of the application. Option C allows the web tier to communicate with the Microsoft SQL Server database running on Amazon EC2 in a private subnet, ensuring that the application has the data it needs to function.

Answer: AC

Question18 : A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.
Which solution will meet these requirements with the LEAST operational overhead?

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

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

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

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

Explanation : Explanation :Amazon Textract is designed for extracting text and data from scanned documents. Amazon Comprehend Medical is a Natural Language Processing (NLP) service that uses machine learning to extract information about medical conditions, medications and treatment outcomes from unstructured text, such as doctors' notes, clinical trial reports etc. So, using both services together will be able to efficiently extract the text from the reports and identify the PHI with the least operational overhead.

Answer: C

Question19 : A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.
What should a solutions architect do to meet these requirements?

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

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

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

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

Explanation : Explanation :Using Spot Instances within an Amazon EKS managed node group would be the best solution for running stateless applications in containers within the AWS Cloud,

as this will minimize cost and operational overhead. Spot Instances are a cost-effective choice for applications that can tolerate disruptions.

Answer: B

Question20 : A company has a data ingestion workflow that consists of the following:
? An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
? An AWS Lambda function to process the data and record metadata
The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.
Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

A: Deploy the Lambda function in multiple Availability Zones.

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

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

D: Increase provisioned throughput for the Lambda function.

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

Explanation : Explanation :Creating an Amazon Simple Queue Service (Amazon SQS) and subscribing it to the SNS topic, and modifying the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue can prevent data loss during network failures. Amazon SQS is a robust queue system which will hold the messages during any interruption and process the data when Lambda function is ready. This combintion ensures that every data is being processed and no data lose even in the case of network problems.

Answer: BE

Question21 : A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability

Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :The question requirement is for only EC2 instances that run in the private subnets to have access to the RDS databases. This can be achieved by creating a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets and attaching the security group to the DB instances.

Answer: C

Question22 : 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?

A: Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.

B: Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.

C: Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the

database in another AWS Region.

D: Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Explanation : Explanation :Migrating the Oracle database to Amazon RDS for Oracle will provide the company with the most recent version of the database. In addition, activating Cross-Region automated backups will replicate the snapshots to another AWS region, thus setting up a disaster recovery solution. This solution also minimizes operational overhead as Amazon RDS manages the database infrastructure.

Answer: B

Question23 : 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?

A: Configure the Lambda function for deployment across multiple Availability Zones.

B: Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.

C: Configure the SNS topic’s retry strategy to increase both the number of retries and the wait time between retries.

D: 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 : Explanation :Configuring an Amazon Simple Queue Service (SQS) queue as the on-failure destination makes use of the built-in resilience and decoupling of the AWS Managed service. This way, if a message (or in the context of this workflow, a notification) can't be processed at the moment of arrival due to a failure in the Lambdas or in the network, it will be stored in the queue and the system will attempt to process it again later. This would ensure that when failure occurs, the corresponding data can be ingested when the system is back online, eliminating the need for the company to manually rerun the job.

Answer: D

Question24 : A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.
Which design should a solutions architect recommend?

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

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

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

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

Explanation : Explanation :Option D allows the company to have the agility of receiving notifications when the database on Amazon RDS is updated. An Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues can effectively distribute the message to multiple target systems. This ensures the information is quickly and effectively disseminated to all necessary targets. And then, updating the targets can be easily achieved by using AWS Lambda functions.

Answer: D

Question25 : A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.
Which set of services should a solutions architect recommend to meet these requirements?

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

B: Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage

C: Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage

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

Explanation : Explanation :Amazon EBS provides the high I/O performance required for video processing. Amazon S3 provides high durability, making it a reasonable choice for storing media files. Amazon S3 Glacier is a cost-efficient solution for long-term storage and suitable for archival storage.

Answer: A

Question26 : 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.)

A: Create an ongoing replication task.

B: Create a database backup of the on-premises database.

C: Create an AWS Database Migration Service (AWS DMS) replication server.

D: Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).

E: Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

Explanation : Explanation :The AWS Database Migration Service (AWS DMS) helps migrate

databases to AWS while keeping the source database in operation during the migration. This process minimizes downtime and allows continuous data replication. DMS is used in combination with ongoing replication tasks to keep the databases synchronised.

Answer: AC

Question27 : 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?

A: 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.

B: 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.

C: 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.

D: 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.

Explanation : Explanation :Amazon CloudFront is a built-in content delivery network (CDN) of AWS, which helps to speed up distribution of static and dynamic web content such as .html, .css, .js, and image files to users all over the world. It works by copying the content of a website to a network of servers spread around the world, and serving content to users from the nearest server. This minimizes the latency, giving users the fastest load times and best response times possible, which matches the design needs given in the question.

Answer: A

Question28 : A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company

has noticed slow application performance and wants to improve the performance as much as possible.
Which solution will meet these requirements with the LEAST operational overhead?

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

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

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

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

Explanation : Explanation :Amazon AppFlow provides a secure, scalable, and efficient way to transfer data between SaaS applications and AWS services, minimizing operational overhead. It also integrates with S3 event notifications and SNS topics for completing notifications, meeting all the requirements without causing too much burden on operations.

Answer: B

Question29 : A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.
What should a solutions architect do to meet these requirements?

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

B: Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.

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

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

Explanation : Explanation :Amazon Rekognition effectively analyzes images and can automatically identify inappropriate content, minimizing the development effort. While Amazon Comprehend is a NLP service more suited for analysing text, not images. Amazon SageMaker and AWS Fargate would involve more development and training to be used for this purpose.

Answer: B

Question30 : A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.
What should a solutions architect do to meet these requirements?

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

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

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

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

Explanation : Explanation :Option A is the best option as it addresses all the requirements stated

in the question. AWS Certificate Manager (ACM) provides easy, no-cost, managed service for creating and managing public SSL/TLS certificates for your AWS-based websites and applications. ACM handles the complexity of creating and managing public SSL/TLS certificates, providing secured network communications and establishing the identity of websites over the Internet. ALB supports native integration with ACM to ease the management and renewal of certificates. ACM also provides automatic renewal and deployment of certificates that eliminates the risk of outages due to expired certificates and reduces the operational complexity of post issuance certificate management.

Answer: A

Question31 : A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A: Configure the application to send the data to Amazon Kinesis Data Firehose.

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

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

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

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

Explanation : Explanation :

Answer: BD

Question32 : A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a

highly available and durable storage solution that preserves how users currently access the files. What should a solutions architect do to meet these requirements?

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

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

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

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

Explanation : Explanation :Amazon FSx for Windows File Server is a fully managed service that provides cost-effective and fully native Microsoft Windows file systems. Extending the file share environment to Amazon FSx for Windows File Server with a multi-AZ configuration will provide high availability and durability and also maintain the same user access experience.

Answer: C

Question33 : A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.
What should a solutions architect do to meet these requirements?

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

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

C: Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

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

Explanation : Explanation :Amazon Elastic Container Service (Amazon ECS) on AWS Fargate is a perfect choice since it allows the company to run containers without having to manage the

underlying infrastructure, thus they will not be responsible for provisioning and managing that. It will also be able to meet the requirements of scalability and availability as Fargate automatically scales and adjusts to the needs of the containerized workload.

Answer: C

Question34 : A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.
What should the company do to guarantee the EC2 capacity?

A: Purchase Reserved Instances that specify the Region needed.

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

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

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

Explanation : Explanation :Creating an On-Demand Capacity Reservation that specifies the Region and three Availability Zones is the appropriate option because it guarantees the capacity in the specific AWS Region and Availability Zones the company needs. Purchasing Reserved Instances only reserves the capacity but doesn't guarantee it, also it does not provide the ability to specify the Availability Zones.

Answer: D

Question35 : A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.
Which solution will meet these requirements with the LEAST operational overhead?

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

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

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

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

Explanation : Explanation :Storing the database credentials as a secret in AWS Secrets Manager, enabling automatic rotation for the secret, and attaching the necessary permissions to the EC2 role provides least operational overhead. AWS Secrets Manager protects access to applications, services, and IT resources. This eliminates the upfront and ongoing investment needed to operate your infrastructure securely.

Answer: C

Question36 : A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.
What should a solutions architect do to ensure messages are being processed once only?

A: Use the CreateQueue API call to create a new queue.

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

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

D: Use the ChangeMessageVisibility API call to increase the visibility timeout.

Explanation : Explanation :ChangeMessageVisibility API call allows one to temporarily block other consumers from receiving and processing the message, thus ensuring single processing and preventing duplication.

Answer: D

Question37 : A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

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

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

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

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

Explanation : Explanation :The question scenario suggests that the company is looking to extend their on-premises infrastructure to AWS with a highly available, low latency connection to an AWS Region, but also wants to minimize costs and accepts slower traffic for failover scenarios. Option A meets these requirements well. It involves provisioning an AWS Direct Connect which provides a high bandwidth, low latency connection to AWS, and provisioning a VPN as a backup. A VPN would cost less than a second Direct Connect and could fulfill the requirement for the slower traffic when the primary Direct Connect fails.

Answer: A

Question38 : A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.
Which solution will meet these requirements with the LEAST operational effort?

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

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

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

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

Explanation : Explanation :Putting the Auto Scaling group across multiple Availability Zones will increase the application's availability, ensuring that even if one zone goes down, the application can still function normally. Using the Multi-AZ feature for the database will also increase its availability and durability, and the use of Amazon RDS Proxy will help manage database connections and offer better security. This solution requires the least operational effort and maximises availability and data protection.

Answer: B

Question39 : A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour.
What should the solutions architect recommend to meet these requirements?

A: Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.

B: Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

C: Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.

D: Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Explanation : Explanation :The need for a solution with an RPO of 15 minutes and an RTO of an hour could be efficiently met by using DynamoDB's point-in-time recovery feature. It allows you to restore your table data to any point in time in the last 35 days, thus providing a good solution for quick recovery in case of data corruption.

Answer: B

Question40 : A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.
How can the solutions architect meet this requirement?

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

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

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

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

Explanation : Explanation :Deploying an S3 VPC gateway endpoint into the VPC and attaching an endpoint policy that allows access to the S3 buckets would provide direct, private connectivity between the VPC and S3, without going through the public internet. This would reduce the data transfer costs.

Answer: D

Question41 : A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs ta share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key

Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots. What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

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

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

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

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

Explanation : Explanation :Option B is the most secure way to share an AMI. It strikes a balance between security and functionality. It only shares the AMI with the MSP Partner's AWS account, reducing access to the AMI, and thus enhancing the security. It also modifies the key policy to allow the MSP Partner's AWS account to use the key, which ensures the MSP Partner can access and use the AMI securely.

Answer: B

Question42 : A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.
Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

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

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

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

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

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

Explanation : Explanation :Option B creates a security group that only allows inbound access from the company's network, enabling the connection from the on-premises network through the company's internet connection. Option D secures the application instances by allowing SSH access only from the bastion host, thus maintaining the security of the private subnet.

Answer: BD

Question43 : A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate. What should a solutions architect recommend to meet this requirement?

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

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

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

D: Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure

the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

Explanation : Explanation :AWS Config allows for the identification of resources that are noncompliant with desired configurations, including certificates expiring within 30 days, and with EventBridge or CloudWatch Events, a custom alert could then be set up to send a notification via Amazon SNS. This approach meets the requirement to alert the security team 30 days before the certificate expires.

Answer: B

Question44 : A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability 10 delete the objects. What should a solutions architect do to meet these requirements?

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

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

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

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

Explanation : Explanation :The solution architect can create an S3 bucket with S3 Object Lock enabled where versioning is also enabled to provide unchangeable objects until the company decides to modify them. By setting a retention period of 100 years and using governance mode as the default retention mode, it ensures that the objects remain unchangeable but allows objects to be overwritten when needed, thus providing the flexibility required by the company.

Answer: B

Question45 : A company wants to reduce the cost of its existing three-tier web architecture. The

web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.
The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.
Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

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

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

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

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

Explanation : Explanation :Reserved Instances provide a significant discount compared to On-Demand Instance pricing and provide a capacity reservation when used in a specific Availability Zone. This would be the most suitable and cost effective solution for production EC2 instances that run 24 hours a day. For the development and test instances which only run for 8 hours a day, On-Demand Instances would be a cost effective solution as you pay for compute capacity by the hour with no long term commitments.

Answer: B

Question46 : A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet.
Which solution will meet these requirements?

A: Configure an S3 gateway endpoint.

B: Create an S3 bucket in a private subnet.

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

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

Explanation : Explanation :Configuring an S3 gateway endpoint in a VPC enables the applications to directly connect to Amazon S3 without leaving the Amazon network, thus meeting the company's security regulations of not allowing traffic to travel across the Internet.

Answer: A

Question47 : A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.
The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.
A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.
Which solution meets these requirements?

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

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

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

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

Explanation : Explanation :The Amazon Aurora MySQL with Multi-AZ Aurora Replicas would help increase the application's elasticity and availability. Moreover, the database cloning would allow the staging database to be created on-demand without affecting the normal operation or causing delays on the usage of the staging environment, which would solve the application latency issue experienced by the users every 4 hours when the full database export is pulled. By implementing this solution architecture, the development team would be able to continue using the staging environment without experiencing any service interruptions or delays.

Answer: B

Question48 : A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.
Which solution will meet these requirements?

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

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

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

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

Explanation : Explanation :Configuring the Requester Pays option on the company's S3 bucket means that the requester, in this case, the European marketing firm, would shoulder the data transfer fees which would help keep the company's data transfer costs low.

Answer: A

Question49 : A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.
Which solution will meet these requirements with the LEAST operational overhead?

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

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

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

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

Explanation : Explanation :This solution meets all the requirements specified in the question by using AWS integrated services. The Amazon API Gateway API can be used to ingest real-time data and Amazon Kinesis data stream will perform real-time processing. Lambda function are serverless and provides an event-driven compute service which enables to run the code and scale automatically. Amazon S3 will be used as the storage solution to store the data.

Answer: C

Question50 : A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years.
What is the MOST operationally efficient solution that meets these requirements?

A: Use DynamoDB point-in-time recovery to back up the table continuously.

B: Use AWS Backup to create backup schedules and retention policies for the table.

C: Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

D: Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an

Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

Explanation : Explanation :AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. In this case, we can use it to automatically backup DynamoDB table and set retention policies to keep the data for 7 years. It offloads the burden of writing custom scripts and manual interventions, thus being the most operationally efficient solution.

Answer: B
