Exam Questions Export

Q1: A medium-sized business has a taxi dispatch application deployed on an Amazon EC2 instance. Because of an unknown bug, the application causes the instance to freeze regularly. Then, the instance has to be manually restarted via the AWS management console. Which of the following is the MOST cost-optimal and resource-efficient way to implement an automated solution until a permanent fix is delivered by the development team?

[ ] Use Amazon EventBridge events to trigger an AWS Lambda function to reboot the instance status every 5 minutes

[CORRECT] Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, an EC2 Reboot CloudWatch Alarm Action can be used to reboot the instance

[ ] Use Amazon EventBridge events to trigger an AWS Lambda function to check the instance status every 5 minutes. In the case of Instance Health Check failure, the AWS lambda function can use Amazon EC2 API to reboot the instance

[ ] Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, Amazon CloudWatch Alarm can publish to an Amazon Simple Notification Service (Amazon SNS) event which can then trigger an AWS lambda function. The AWS lambda function can use Amazon EC2 API to reboot the instance

Q2: You have built an application that is deployed with Elastic Load Balancing and an Auto Scaling Group. As a Solutions Architect, you have configured aggressive Amazon CloudWatch alarms, making your Auto Scaling Group (ASG) scale in and out very quickly, renewing your fleet of Amazon EC2 instances on a daily basis. A production bug appeared two days ago, but the team is unable to SSH into the instance to debug the issue, because the instance has already been terminated by the Auto Scaling Group. The log files are saved on the Amazon EC2 instance. How will you resolve the issue and make sure it doesn't happen again?

[CORRECT] Install an Amazon CloudWatch Logs agents on the Amazon EC2 instances to send logs to Amazon CloudWatch

[ ] Use AWS Lambda to regularly SSH into the Amazon EC2 instances and copy the log files to Amazon S3

[ ] Disable the Termination from the Auto Scaling Group any time a user reports an issue

[ ] Make a snapshot of the Amazon EC2 instance just before it gets terminated

Q3: An application hosted on Amazon EC2 contains sensitive personal information about all its customers and needs to be protected from all types of cyber-attacks. The company is considering using the AWS Web Application Firewall (AWS WAF) to handle this requirement. Can you identify the correct solution leveraging the capabilities of AWS WAF?

[ ] Configure an Application Load Balancer (ALB) to balance the workload for all the Amazon EC2 instances. Configure Amazon CloudFront to distribute from an Application Load Balancer since AWS WAF cannot be directly configured on ALB. This configuration not only provides necessary safety but is scalable too

[ ] AWS WAF can be directly configured on Amazon EC2 instances for ensuring the security of the underlying application data

[CORRECT] Create Amazon CloudFront distribution for the application on Amazon EC2 instances. Deploy AWS WAF on Amazon CloudFront to provide the necessary safety measures

[ ] AWS WAF can be directly configured only on an Application Load Balancer or an Amazon API Gateway. One of these two services can then be configured with Amazon EC2 to build the needed secure architecture

Q4: A company wants to ensure high availability for its Amazon RDS database. The development team wants to opt for Multi-AZ deployment and they would like to understand what happens when the primary instance of the Multi-AZ configuration goes down. As a Solutions Architect, which of the following will you identify as the outcome of the scenario?

[ ] The application will be down until the primary database has recovered itself

[ ] The URL to access the database will change to the standby database

[ ] An email will be sent to the System Administrator asking for manual intervention

[CORRECT] The CNAME record will be updated to point to the standby database

Q5: A healthcare startup runs a lightweight reporting application on a single Amazon EC2 On-Demand instance. The application is designed to be stateless, fault-tolerant, and optimized for fast rendering of analytics dashboards. During major health events or news cycles, the team observes latency issues and occasional 5xx errors due to traffic spikes. To meet growing demand without over-provisioning resources during off-peak hours, the company wants to implement a cost-effective, scalable solution that ensures consistent performance even under unpredictable load. Which approach best meets the requirements while minimizing costs?

[ ] Configure an Amazon EventBridge rule to monitor system-level metrics from the EC2 instance. Trigger a Lambda function to re-deploy the application in a different Availability Zone when CPU utilization exceeds 70%

[ ] Clone the EC2 instance using an AMI and launch a second On-Demand instance. Register both instances with an Application Load Balancer to distribute incoming traffic evenly

[ ] Containerize the application using Amazon ECS with Fargate launch type. Deploy the container to a single Fargate task and set a CloudWatch alarm to increase memory and CPU allocation dynamically based on load

[CORRECT] Build an Amazon Machine Image (AMI) from the existing EC2 instance and configure a launch template. Create an Auto Scaling group using the launch template with Spot Instance pricing enabled. Attach an Application Load Balancer to distribute traffic across dynamically launched instances

Q6: While troubleshooting, a cloud architect realized that the Amazon EC2 instance is unable to connect to the internet using the Internet Gateway. Which conditions should be met for internet connectivity to be established? (Select two)

[CORRECT] The network access control list (network ACL) associated with the subnet must have rules to allow inbound and outbound traffic

[ ] The subnet has been configured to be public and has no access to the internet

[ ] The instance's subnet is not associated with any route table

[CORRECT] The route table in the instance's subnet should have a route to an Internet Gateway

[ ] The instance's subnet is associated with multiple route tables with conflicting configurations

Q7: A digital content production company has transitioned all of its media assets to Amazon S3 in an effort to reduce storage costs. However, the rendering engine used in production continues to run in an on-premises data center and requires frequent and low-latency access to large media files. The company wants to implement a storage solution that maintains application performance while keeping costs low. Which approach should the company choose to meet these requirements in the most cost-effective way?

[ ] Use Mountpoint for Amazon S3 on the on-premises rendering servers to facilitate low-latency access to the S3 bucket

[CORRECT] Set up an Amazon S3 File Gateway to provide storage for the on-premises application

[ ] Deploy an Amazon FSx for Lustre file system and sync media data from Amazon S3 into it using DataSync. Mount the FSx file system on the on-premises render servers using a VPN tunnel

[ ] Set up a dedicated on-premises storage array that periodically fetches data from Amazon S3 using a custom-built application. Mount this storage volume on the rendering servers as their primary working directory

Q8: The content division at a digital media agency has an application that generates a large number of files on Amazon S3, each approximately 10 megabytes in size. The agency mandates that the files be stored for 5 years before they can be deleted. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days. The files contain critical business data that is not easy to reproduce, therefore, immediate accessibility is always required. Which solution is the MOST cost-effective for the given use case?

[ ] Set up an Amazon S3 bucket lifecycle policy to move files from Amazon S3 Standard to Amazon S3 Glacier Flexible Retrieval 30 days after object creation. Delete the files 5 years after object creation

[CORRECT] Set up an Amazon S3 bucket lifecycle policy to move files from Amazon S3 Standard to Amazon S3 Standard-IA 30 days after object creation. Delete the files 5 years after object creation

[ ] Set up an Amazon S3 bucket lifecycle policy to move files from Amazon S3 Standard to Amazon S3 One Zone-IA 30 days after object creation. Delete the files 5 years after object creation

[ ] Set up an Amazon S3 bucket lifecycle policy to move files from Amazon S3 Standard to Amazon S3 Standard-IA 30 days after object creation. Archive the files to Amazon S3 Glacier Deep Archive 5 years after object creation

Q9: A digital media startup allows users to submit images through its web portal. These images are uploaded directly into an Amazon S3 bucket. On average, around 200 images are uploaded daily. The company wants to automatically generate a smaller preview version (thumbnail) of each new image and store the resulting thumbnails in a separate Amazon S3 bucket. The team prefers a design that is low-cost, requires minimal infrastructure management, and automatically reacts to new uploads. Which solution will meet these requirements MOST cost-effectively?

[ ] Enable Amazon S3 Access Analyzer and configure it to call an AWS Lambda function whenever a new image is added. Use the Lambda function to generate and store the thumbnail

[CORRECT] Configure the S3 bucket to send an event notification to an AWS Lambda function each time a new image is uploaded. Use the Lambda function to process the image, create a thumbnail, and store the thumbnail in the second S3 bucket

[ ] Set up a step-based processing workflow using AWS Glue jobs triggered on a regular interval. Use the jobs to scan the primary S3 bucket for new files and generate thumbnails for any that lack them. Write the thumbnails to a second S3 bucket

[ ] Deploy a containerized application on AWS Fargate that polls the S3 bucket every minute to detect new uploads. Configure the container to generate thumbnails and save them in the second bucket

Q10: A digital publishing platform stores large volumes of media assets (such as images and documents) in an Amazon S3 bucket. These assets are accessed frequently during business hours by internal editors and content delivery tools. The company has strict encryption policies and currently uses AWS KMS to handle server-side encryption. The cloud operations team notices that AWS KMS request costs are increasing significantly due to the high frequency of object uploads and accesses. The team is now looking for a way to maintain the same encryption method but reduce the cost of KMS usage, especially for frequent access patterns. Which solution meets the company's encryption and cost optimization goals?

[CORRECT] Enable S3 Bucket Keys for server-side encryption with AWS KMS (SSE-KMS) so that new objects use a bucket-level key rather than requesting individual KMS data keys for every object

[ ] Switch to server-side encryption using Amazon S3 managed keys (SSE-S3) to eliminate all AWS KMS-related encryption charges while maintaining the same level of encryption control

[ ] Configure a VPC endpoint for S3 and restrict access to the bucket to traffic originating from the endpoint to avoid additional KMS charges

[ ] Use client-side encryption by generating a local symmetric key and uploading it to Amazon S3 along with each object's metadata for decryption

Q11: An e-commerce company uses a two-tier architecture with application servers in the public subnet and an Amazon RDS MySQL DB in a private subnet. The development team can use a bastion host in the public subnet to access the MySQL database and run queries from the bastion host. However, end-users are reporting application errors. Upon inspecting application logs, the team notices several "could not connect to server: connection timed out" error messages. Which of the following options represent the root cause for this issue?

[ ] The database user credentials (username and password) configured for the application are incorrect

[ ] The database user credentials (username and password) configured for the application do not have the required privilege for the given database

[CORRECT] The security group configuration for the database instance does not have the correct rules to allow inbound connections from the application servers

[ ] The security group configuration for the application servers does not have the correct rules to allow inbound connections from the database instance

Q12: A biomedical research firm operates a file exchange system for external research partners to upload and download experimental data. Currently, the system runs on two Amazon EC2 Linux instances, each configured with Elastic IP addresses to allow access from trusted IPs. File transfers use the SFTP protocol, and Linux user accounts are manually provisioned to enforce file-level access control. Data is stored on a shared file system mounted to both EC2 instances. The firm wants to modernize the solution to a fully managed, serverless model with high IOPS, fine-grained user permission control, and strict IP-based access restrictions. They also want to reduce operational overhead without sacrificing performance or security. Which solution best meets these requirements?

[ ] Use Amazon S3 with server-side encryption enabled. Create an AWS Transfer Family SFTP endpoint with a VPC endpoint in a private subnet. Restrict access to known IPs using security group rules. Manage user-level permissions using IAM role-based access mappings

[ ] Use Amazon FSx for Lustre as the backend storage. Create an AWS Transfer Family SFTP service with a public endpoint. Configure IAM policies to manage user access and attach a security group that restricts access to trusted IP addresses

[ ] Use AWS Storage Gateway in file gateway mode to expose an NFS file share. Deploy AWS Transfer Family with a public endpoint and map user identities using IAM roles. Configure IP allow lists using AWS WAF

[CORRECT] Use Amazon EFS with encryption enabled. Create an AWS Transfer Family SFTP endpoint in a VPC with Elastic IP addresses. Restrict access using a security group that allows traffic only from known IPs. Manage user access using POSIX identity mappings and IAM policies

Q13: An organization operates a legacy reporting tool hosted on an Amazon EC2 instance located within a public subnet of a VPC. This tool aggregates scanned PDF reports from field devices and temporarily stores them on an attached Amazon EBS volume. At the end of each day, the tool transfers the accumulated files to an Amazon S3 bucket for archival. A solutions architect identifies that the files are being uploaded over the internet using S3's public endpoint. To improve security and avoid exposing data traffic to the public internet, the architect needs to reconfigure the setup so that uploads to Amazon S3 occur privately without using the public S3 endpoint. Which solution will fulfill these requirements?

[ ] Create an S3 access point within the same Region and attach a policy that grants the EC2 instance access. Update the application to use the access point alias to upload data

[CORRECT] Create a gateway VPC endpoint for Amazon S3 in the VPC. Ensure that the EC2 instance's subnet route table is updated to route S3 traffic through the endpoint. Confirm that appropriate IAM policies are in place to permit access via the VPC endpoint

[ ] Provision a dedicated AWS Direct Connect link to route traffic from the VPC to Amazon S3 privately

[ ] Set up a NAT gateway in the public subnet and modify the route table of the EC2 instance's subnet to direct Amazon S3 traffic through the NAT gateway

Q14: A fintech company currently operates a real-time search and analytics platform on-premises. This platform ingests streaming data from multiple data-producing systems and provides immediate search capabilities and interactive visualizations for end users. As part of its cloud migration strategy, the company wants to rearchitect the solution using AWS-native services. Which of the following represents the most efficient solution?

[ ] Use AWS Glue streaming ETL to process data streams and load the data into Amazon Redshift. Use Amazon Redshift's full-text search capabilities for querying. Use Amazon QuickSight for data visualizations

[ ] Deploy Amazon EC2 instances to handle the ingestion and processing of streaming data, storing the results in Amazon S3. Utilize Amazon Athena to search the stored data, and use Amazon Managed Grafana to generate dashboards and visual insights

[ ] Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate to ingest the data into Amazon DynamoDB to facilitate full text search. Use Amazon CloudWatch to create dashboards and query the data

[CORRECT] Ingest and process the streaming data using Amazon Kinesis Data Streams, then index the data with Amazon OpenSearch Service for real-time search capabilities. Use Amazon QuickSight to build interactive dashboards and visualizations based on the indexed data

Q15: A global e-commerce platform currently operates its order processing system in a single on-premises data center located in Europe. As the company grows its customer base across Asia and North America, it plans to deploy the application across multiple AWS Regions to improve availability and reduce latency. The company requires that updates to the central order database be completed in under one second with global consistency. The application layer will be deployed separately in each Region, but the order management data must remain centrally managed and globally synchronized. Which solution should a solutions architect recommend to meet these requirements?

[ ] Use Amazon Aurora database with MySQL engine, and configure read-only nodes in other Regions to handle local traffic while routing all write operations to the central Region

[ ] Use Amazon Neptune to store tracking updates as graph data. Deploy clusters in each Region and replicate changes using custom-built Lambda functions and Amazon SQS.

[ ] Use Amazon RDS for MySQL with a cross-Region read replica. Route all writes to the primary Region and use read replicas for local access in other Regions

[CORRECT] Migrate the order data to Amazon DynamoDB and create a global table. Deploy the application in each Region and connect to the local DynamoDB replica for low-latency access

Q16: A financial services company runs its flagship web application on AWS. The application serves thousands of users during peak hours. The company needs a scalable near-real-time solution to share hundreds of thousands of financial transactions with multiple internal applications. The solution should also remove sensitive details from the transactions before storing the cleansed transactions in a document database for low-latency retrieval. As an AWS Certified Solutions Architect Associate, which of the following would you recommend?

[ ] Feed the streaming transactions into Amazon Kinesis Data Firehose. Leverage AWS Lambda integration to remove sensitive data from every transaction and then store the cleansed transactions in Amazon DynamoDB. The internal applications can consume the raw transactions off the Amazon Kinesis Data Firehose

[ ] Batch process the raw transactions data into Amazon S3 flat files. Use S3 events to trigger an AWS Lambda function to remove sensitive data from the raw transactions in the flat file and then store the cleansed transactions in Amazon DynamoDB. Leverage DynamoDB Streams to share the transactions data with the internal applications

[ ] Persist the raw transactions into Amazon DynamoDB. Configure a rule in Amazon DynamoDB to update the transaction by removing sensitive data whenever any new raw transaction is written. Leverage Amazon DynamoDB Streams to share the transactions data with the internal applications

[CORRECT] Feed the streaming transactions into Amazon Kinesis Data Streams. Leverage AWS Lambda integration to remove sensitive data from every transaction and then store the cleansed transactions in Amazon DynamoDB. The internal applications can consume the raw transactions off the Amazon Kinesis Data Stream

Q17: A company's cloud architect has set up a solution that uses Amazon Route 53 to configure the DNS records for the primary website with the domain pointing to the Application Load Balancer (ALB). The company wants a solution where users will be directed to a static error page, configured as a backup, in case of unavailability of the primary website. Which configuration will meet the company's requirements, while keeping the changes to a bare minimum?

[ ] Use Amazon Route 53 Latency-based routing. Create a latency record to point to the Amazon S3 bucket that holds the error page to be displayed

[ ] Use Amazon Route 53 Weighted routing to give minimum weight to Amazon S3 bucket that holds the error page to be displayed. In case of primary failure, the requests get routed to the error page

[CORRECT] Set up Amazon Route 53 active-passive type of failover routing policy. If Amazon Route 53 health check determines the Application Load Balancer endpoint as unhealthy, the traffic will be diverted to a static error page, hosted on Amazon S3 bucket

[ ] Set up Amazon Route 53 active-active type of failover routing policy. If Amazon Route 53 health check determines the Application Load Balancer endpoint as unhealthy, the traffic will be diverted to a static error page, hosted on Amazon S3 bucket

Q18: A retail enterprise is expanding its hybrid IT infrastructure and plans to securely connect its on-premises corporate network to its AWS environment. The company wants to ensure that all data exchanged between on-premises systems and AWS is encrypted at both the network and session layers. Additionally, the solution must incorporate granular security controls that restrict unnecessary or unauthorized access between the cloud and on-premises environments. A solutions architect must recommend a scalable and secure approach that supports these goals. Which solution best meets these requirements?

[CORRECT] Set up AWS Site-to-Site VPN to connect the on-premises network to the AWS VPC. Use route tables to manage traffic flow and configure security groups and network ACLs to allow only authorized communication between systems

[ ] Establish a dedicated AWS Direct Connect connection between the corporate network and AWS. Configure VPC route tables to control traffic flow and use security groups and network ACLs to restrict access as needed

[ ] Use AWS Client VPN to allow corporate users to connect to the VPC individually. Manage access controls with security groups and IAM policies

[ ] Set up a bastion host in a public subnet of the VPC to provide SSH-based access to AWS resources from the corporate network. Use security groups to control access

Q19: A company needs a massive PostgreSQL database and the engineering team would like to retain control over managing the patches, version upgrades for the database, and consistent performance with high IOPS. The team wants to install the database on an Amazon EC2 instance with the optimal storage type on the attached Amazon EBS volume. As a solutions architect, which of the following configurations would you suggest to the engineering team?

[CORRECT] Amazon EC2 with Amazon EBS volume of Provisioned IOPS SSD (io1) type

[ ] Amazon EC2 with Amazon EBS volume of Throughput Optimized HDD (st1) type

[ ] Amazon EC2 with Amazon EBS volume of cold HDD (sc1) type

[ ] Amazon EC2 with Amazon EBS volume of General Purpose SSD (gp2) type

Q20: A medical devices company uses Amazon S3 buckets to store critical data. Hundreds of buckets are used to keep the data segregated and well organized. Recently, the development team noticed that the lifecycle policies on the Amazon S3 buckets have not been applied optimally, resulting in higher costs. As a Solutions Architect, can you recommend a solution to reduce storage costs on Amazon S3 while keeping the IT team's involvement to a minimum?

[ ] Configure Amazon EFS to provide a fast, cost-effective and sharable storage service

[ ] Use Amazon S3 One Zone-Infrequent Access, to reduce the costs on Amazon S3 storage

[ ] Use Amazon S3 Outposts storage class to reduce the costs on Amazon S3 storage by storing the data on-premises

[CORRECT] Use Amazon S3 Intelligent-Tiering storage class to optimize the Amazon S3 storage costs

Q21: Computer vision researchers at a university are trying to optimize the I/O bound processes for a proprietary algorithm running on Amazon EC2 instances. The ideal storage would facilitate high-performance IOPS when doing file processing in a temporary storage space before uploading the results back into Amazon S3. As a solutions architect, which of the following AWS storage options would you recommend as the MOST performant as well as cost-optimal?

[ ] Use Amazon EC2 instances with Amazon EBS General Purpose SSD (gp2) as the storage option

[ ] Use Amazon EC2 instances with Amazon EBS Throughput Optimized HDD (st1) as the storage option

[ ] Use Amazon EC2 instances with Amazon EBS Provisioned IOPS SSD (io1) as the storage option

[CORRECT] Use Amazon EC2 instances with Instance Store as the storage option

Q22: The infrastructure team at a company maintains 5 different VPCs (let's call these VPCs A, B, C, D, E) for resource isolation. Due to the changed organizational structure, the team wants to interconnect all VPCs together. To facilitate this, the team has set up VPC peering connection between VPC A and all other VPCs in a hub and spoke model with VPC A at the center. However, the team has still failed to establish connectivity between all VPCs. As a solutions architect, which of the following would you recommend as the MOST resource-efficient and scalable solution?

[CORRECT] Use AWS transit gateway to interconnect the VPCs

[ ] Use an internet gateway to interconnect the VPCs

[ ] Establish VPC peering connections between all VPCs

[ ] Use a VPC endpoint to interconnect the VPCs

Q23: A logistics company runs a two-step job handling process on AWS. The first step quickly receives job submissions from clients, while the second step requires longer processing time to complete each job. Currently, both steps run on separate Amazon EC2 Auto Scaling groups. However, during high-demand hours, the job processing stage falls behind, and there is concern that jobs may be lost due to instance termination during scaling events. A solutions architect needs to design a more scalable and reliable architecture that preserves job data and accommodates fluctuating demand in both stages. Which solution will meet these requirements?

[CORRECT] Set up two Amazon SQS queues to decouple the job intake and job processing stages respectively. Assign one SQS queue to collect incoming jobs, and another to queue them for processing. Configure the EC2 instances to poll the relevant queue. Scale the Auto Scaling groups based on number of messages in each queue

[ ] Set up a single Amazon SQS queue for both the job intake and job processing stages. Assign the SQS queue to collect incoming jobs as well as processing jobs. Configure all EC2 instances to poll this queue. Scale the Auto Scaling groups based on number of messages in the queue

[ ] Configure each Auto Scaling group to maintain its maximum expected size during peak hours by setting a fixed minimum capacity. Monitor CPUUtilization through Amazon CloudWatch to ensure consistent scaling behavior

[ ] Set up two Amazon SQS queues to decouple the job intake and job processing stages respectively. Assign one SQS queue to collect incoming jobs, and another to queue them for processing. Configure the EC2 instances to poll the relevant queue. Scale the Auto Scaling groups based on notifications from each queue

Q24: A media company is evaluating the possibility of moving its IT infrastructure to the AWS Cloud. The company needs at least 10 terabytes of storage with the maximum possible I/O performance for processing certain files which are mostly large videos. The company also needs close to 450 terabytes of very durable storage for storing media content and almost double of it, i.e. 900 terabytes for archival of legacy data. As a Solutions Architect, which set of services will you recommend to meet these requirements?

[ ] Amazon EC2 instance store for maximum performance, AWS Storage Gateway for on-premises durable data access and Amazon S3 Glacier Deep Archive for archival storage

[CORRECT] Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

[ ] Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

[ ] Amazon S3 standard storage for maximum performance, Amazon S3 Intelligent-Tiering for intelligent, durable storage, and Amazon S3 Glacier Deep Archive for archival storage

Q25: A global enterprise is modernizing its hybrid IT infrastructure to improve both availability and network performance. The company operates a TCP-based application hosted on Amazon EC2 instances that are deployed across multiple AWS Regions, while a secondary UDP-based component of the application is hosted in its on-premises data centers. These application components must be accessed by customers around the world with minimal latency and consistent uptime. Which combination of options should a solutions architect implement for the given use case? (Select two)

[CORRECT] Configure an AWS Global Accelerator standard accelerator, and register the TCP-based EC2 workloads behind the load balancers

[ ] Create a Network Load Balancer (NLB) in each Region to handle the EC2-based TCP traffic. For the UDP-based on-premises workload, configure Application Load Balancers in each Region to route to the on-premises endpoints via IP-based target groups

[ ] Set up AWS Direct Connect connections to route all TCP and UDP traffic through a single Region, using static routes and BGP failover

[CORRECT] Create a Network Load Balancer (NLB) in each Region to handle the EC2-based TCP traffic. For the UDP-based on-premises workload, configure NLBs in each Region to route to the on-premises endpoints via IP-based target groups

[ ] Deploy AWS PrivateLink to connect each on-premises UDP workload to the AWS Regions through interface endpoints exposed by the Network Load Balancers

Q26: A SaaS analytics company is deploying a microservices-based application on Amazon ECS using the Fargate launch type. The application requires access to a shared, POSIX-compliant file system that is available across multiple Availability Zones for redundancy and availability. To meet compliance requirements, the system must support regional backups and cross-Region data recovery with a recovery point objective (RPO) of no more than 8 hours. A backup strategy will be implemented using AWS Backup to automate replication across Regions. As the lead cloud architect, you are evaluating file storage solutions that align with these requirements. Which option best meets the application's availability, durability, and RPO objectives?

[ ] Use Amazon FSx for NetApp ONTAP with a Multi-AZ deployment and rely on its native high availability and AWS Backup integration to replicate the file system to another Region automatically

[ ] Deploy Amazon FSx for Lustre and configure a backup plan using AWS Backup for cross-Region replication of the file system metadata

[ ] Configure Amazon S3 with the S3 Standard storage class and mount it in containers using Mountpoint for Amazon S3. Use AWS Backup to replicate objects to another Region

[CORRECT] Use Amazon Elastic File System (Amazon EFS) with the Standard storage class and configure AWS Backup to create cross-Region backups on a scheduled basis

Q27: Reporters at a news agency upload/download video files (about 500 megabytes each) to/from an Amazon S3 bucket as part of their daily work. As the agency has started offices in remote locations, it has resulted in poor latency for uploading and accessing data to/from the given Amazon S3 bucket. The agency wants to continue using a serverless storage solution such as Amazon S3 but wants to improve the performance. As a solutions architect, which of the following solutions do you propose to address this issue? (Select two)

[CORRECT] Use Amazon CloudFront distribution with origin as the Amazon S3 bucket. This would speed up uploads as well as downloads for the video files

[ ] Create new Amazon S3 buckets in every region where the agency has a remote office, so that each office can maintain its storage for the media assets

[ ] Move Amazon S3 data into Amazon Elastic File System (Amazon EFS) created in a US region, connect to Amazon EFS file system from Amazon EC2 instances in other AWS regions using an inter-region VPC peering connection

[ ] Spin up Amazon EC2 instances in each region where the agency has a remote office. Create a daily job to transfer Amazon S3 data into Amazon EBS volumes attached to the Amazon EC2 instances

[CORRECT] Enable Amazon S3 Transfer Acceleration (Amazon S3TA) for the Amazon S3 bucket. This would speed up uploads as well as downloads for the video files

Q28: A financial auditing firm uses Amazon S3 to store sensitive client records that are subject to write-once-read-many (WORM) regulations to prevent alteration or deletion of records for a specific retention period. The firm wants to enforce immutable storage, such that even administrators cannot overwrite or delete the records during the lock duration. They also need audit-friendly enforcement to prevent accidental or malicious deletion. Which configuration of S3 Object Lock will ensure that the retention policy is strictly enforced, and no user (including root or administrators) can override or delete protected objects during the lock period?

[CORRECT] Use S3 Object Lock in Compliance Mode, which enforces retention policies strictly and prevents all users from modifying or deleting data during the retention period

[ ] Use S3 Lifecycle Policies to transition data to Glacier Deep Archive and treat it as immutable during the archival period

[ ] Enable S3 Versioning and set a bucket policy that denies s3:DeleteObject to all users during the retention period

[ ] Use S3 Object Lock in Governance Mode, which allows only IAM users with elevated permissions to override or remove retention settings

Q29: A pharmaceutical company is considering moving to AWS Cloud to accelerate the research and development process. Most of the daily workflows would be centered around running batch jobs on Amazon EC2 instances with storage on Amazon Elastic Block Store (Amazon EBS) volumes. The CTO is concerned about meeting HIPAA compliance norms for sensitive data stored on Amazon EBS. Which of the following options outline the correct capabilities of an encrypted Amazon EBS volume? (Select three)

[ ] Data at rest inside the volume is NOT encrypted

[ ] Any snapshot created from the volume is NOT encrypted

[CORRECT] Data moving between the volume and the instance is encrypted

[CORRECT] Any snapshot created from the volume is encrypted

[ ] Data moving between the volume and the instance is NOT encrypted

[CORRECT] Data at rest inside the volume is encrypted

Q30: A retail company maintains an AWS Direct Connect connection to AWS and has recently migrated its data warehouse to AWS. The data analysts at the company query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 60 megabytes and the query responses returned by the data warehouse are not cached in the visualization tool. Each webpage returned by the visualization tool is approximately 600 kilobytes. Which of the following options offers the LOWEST data transfer egress cost for the company?

[ ] Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over the internet at a location in the same region

[CORRECT] Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over a Direct Connect connection at a location in the same region

[ ] Deploy the visualization tool on-premises. Query the data warehouse directly over an AWS Direct Connect connection at a location in the same AWS region

[ ] Deploy the visualization tool on-premises. Query the data warehouse over the internet at a location in the same AWS region

Q31: An enterprise is developing an internal compliance framework for its cloud infrastructure hosted on AWS. The enterprise uses AWS Organizations to group accounts under various organizational units (OUs) based on departmental function. As part of its governance controls, the security team mandates that all Amazon EC2 instances must be tagged to indicate the level of data classification — either 'confidential' or 'public'. Additionally, the organization must ensure that IAM users cannot launch EC2 instances without assigning a classification tag, nor should they be able to remove the tag from running instances. A solutions architect must design a solution to meet these compliance controls while minimizing operational overhead. Which combination of steps will meet these requirements? (Select two)

[CORRECT] Create a service control policy (SCP) that denies the ec2:RunInstances API action unless the required tag key is present in the request. Create a second SCP that denies the ec2:DeleteTags action for EC2 resources. Attach both SCPs to the relevant OU in AWS Organizations

[ ] Enable AWS Config rules to detect noncompliant EC2 instances. Trigger an AWS Systems Manager Automation runbook to reapply missing tags automatically when noncompliance is detected

[CORRECT] Define a tag policy in AWS Organizations that enforces the dataClassification key and restricts values to 'confidential' and 'public'. Attach this tag policy to the applicable organizational unit (OU) to enforce uniform tagging behavior across accounts

[ ] Use AWS Identity and Access Management (IAM) permission boundaries to restrict EC2-related actions unless the dataClassification tag is present. Apply these boundaries to all IAM roles used for EC2 provisioning

[ ] Create a tag enforcement Lambda function that runs on a schedule to identify EC2 instances without the required tag. The function sends a notification to administrators and optionally shuts down noncompliant resources

Q32: A financial data processing company runs a workload on Amazon EC2 instances that fetch and process real-time transaction batches from an Amazon SQS queue. The application needs to scale based on unpredictable message volume, which fluctuates significantly throughout the day. The system must process messages with minimal delay and no downtime, even during peak spikes. The company is seeking a solution that balances cost-efficiency with availability and elasticity. Which EC2 purchasing strategy best meets these requirements in the most cost-effective manner?

[ ] Use EC2 Reserved Instances for the baseline workload and configure EC2 Auto Scaling to launch On-Demand Instances for all traffic spikes

[CORRECT] Use Reserved Instances for the baseline level of traffic and configure EC2 Auto Scaling with Spot Instances to handle spikes in message volume

[ ] Purchase EC2 Reserved Instances to match peak capacity and assign all message processing tasks to these instances regardless of load variations

[ ] Use EC2 Spot Instances exclusively with Auto Scaling enabled to match message volume fluctuations and save on compute costs

Q33: A Customer relationship management (CRM) application is facing user experience issues with users reporting frequent sign-in requests from the application. The application is currently hosted on multiple Amazon EC2 instances behind an Application Load Balancer. The engineering team has identified the root cause as unhealthy servers causing session data to be lost. The team would like to implement a distributed in-memory cache-based session management solution. As a solutions architect, which of the following solutions would you recommend?

[ ] Use Amazon DynamoDB for distributed in-memory cache based session management

[CORRECT] Use Amazon Elasticache for distributed in-memory cache based session management

[ ] Use Amazon RDS for distributed in-memory cache based session management

[ ] Use Application Load Balancer sticky sessions

Q34: An application with global users across AWS Regions had suffered an issue when the Elastic Load Balancing (ELB) in a Region malfunctioned thereby taking down the traffic with it. The manual intervention cost the company significant time and resulted in major revenue loss. What should a solutions architect recommend to reduce internet latency and add automatic failover across AWS Regions?

[CORRECT] Set up AWS Global Accelerator and add endpoints to cater to users in different geographic locations

[ ] Set up AWS Direct Connect as the backbone for each of the AWS Regions where the application is deployed

[ ] Create Amazon S3 buckets in different AWS Regions and configure Amazon CloudFront to pick the nearest edge location to the user

[ ] Set up an Amazon Route 53 geoproximity routing policy to route traffic

Q35: A tech company runs a web application that includes multiple internal services deployed across Amazon EC2 instances within a VPC. These services require communication with a third-party SaaS provider's API for analytics and billing, which is also hosted on the AWS infrastructure. The company is concerned about minimizing public internet exposure while maintaining secure and reliable connectivity. The solution must ensure private access without allowing unsolicited incoming traffic from the SaaS provider. Which solution will best meet these requirements?

[CORRECT] Use AWS PrivateLink to create a private endpoint within the application's VPC that connects securely to the SaaS provider's VPC

[ ] Establish a VPN connection using AWS Site-to-Site VPN to create a secure tunnel between the internal services and the third-party SaaS provider

[ ] Set up VPC peering between the application VPC and the SaaS provider's VPC to allow direct communication

[ ] Use AWS CloudFront to route requests from the application's internal services to the SaaS provider through edge locations

Q36: A health-care company manages its web application on Amazon EC2 instances running behind Auto Scaling group (ASG). The company provides ambulances for critical patients and needs the application to be reliable. The workload of the company can be managed on 2 Amazon EC2 instances and can peak up to 6 instances when traffic increases. As a Solutions Architect, which of the following configurations would you select as the best fit for these requirements?

[ ] The Auto Scaling group should be configured with the minimum capacity set to 2, with 1 instance each in two different Availability Zones. The maximum capacity of the Auto Scaling group should be set to 6

[ ] The Auto Scaling group should be configured with the minimum capacity set to 2 and the maximum capacity set to 6 in a single Availability Zone

[ ] The Auto Scaling group should be configured with the minimum capacity set to 4, with 2 instances each in two different AWS Regions. The maximum capacity of the Auto Scaling group should be set to 6

[CORRECT] The Auto Scaling group should be configured with the minimum capacity set to 4, with 2 instances each in two different Availability Zones. The maximum capacity of the Auto Scaling group should be set to 6

Q37: A mobile-based e-learning platform is migrating its backend storage layer to Amazon DynamoDB to support a rapidly increasing number of student users and learning transactions. The platform must ensure seamless availability and minimal disruption for a global user base. The DynamoDB design must provide low-latency performance, high availability, and automatic fault tolerance across geographies with the lowest possible operational overhead and cost. Which solution will fulfill these needs in the most cost-efficient manner?

[ ] Deploy separate DynamoDB tables in each required AWS Region using on-demand capacity mode. Implement a custom cross-Region replication mechanism by streaming data changes with DynamoDB Streams and processing them through AWS Lambda functions

[ ] Enable DynamoDB Accelerator (DAX) to reduce response time for read operations. Deploy DAX in one Region, and use scheduled Lambda functions to replicate data to other Regions

[CORRECT] Use DynamoDB global tables for automatic multi-Region replication. Enable provisioned capacity mode with auto scaling to optimize cost and ensure consistent availability

[ ] Create separate DynamoDB tables in multiple Regions. Use AWS Data Pipeline to synchronize data periodically between Regions to maintain availability

Q38: A company hires experienced specialists to analyze the customer service calls attended by its call center representatives. Now, the company wants to move to AWS Cloud and is looking at an automated solution to analyze customer service calls for sentiment analysis via ad-hoc SQL queries. As a Solutions Architect, which of the following solutions would you recommend?

[ ] Use Amazon Kinesis Data Streams to read the audio files and Amazon Alexa to convert them into text. Amazon Kinesis Data Analytics can be used to analyze these files and Amazon Quicksight can be used to visualize and display the output

[CORRECT] Use Amazon Transcribe to convert audio files to text and Amazon Athena to perform SQL based analysis to understand the underlying customer sentiments

[ ] Use Amazon Transcribe to convert audio files to text and Amazon Quicksight to perform SQL based analysis on these text files to understand the underlying patterns. Visualize and display them onto user Dashboards for reporting purposes

[ ] Use Amazon Kinesis Data Streams to read the audio files and machine learning (ML) algorithms to convert the audio files into text and run customer sentiment analysis

Q39: A streaming solutions company is building a video streaming product by using an Application Load Balancer (ALB) that routes the requests to the underlying Amazon EC2 instances. The engineering team has noticed a peculiar pattern. The Application Load Balancer removes an instance from its pool of healthy instances whenever it is detected as unhealthy but the Auto Scaling group fails to kick-in and provision the replacement instance. What could explain this anomaly?

[ ] Both the Auto Scaling group and Application Load Balancer are using ALB based health check

[ ] Both the Auto Scaling group and Application Load Balancer are using Amazon EC2 based health check

[ ] The Auto Scaling group is using ALB based health check and the Application Load Balancer is using Amazon EC2 based health check

[CORRECT] The Auto Scaling group is using Amazon EC2 based health check and the Application Load Balancer is using ALB based health check

Q40: A fintech company recently conducted a security audit and discovered that some IAM roles and Amazon S3 buckets might be unintentionally shared with external accounts or publicly accessible. The security team wants to identify these overly permissive resources and ensure that only intended principals (within their AWS Organization or specific AWS accounts) have access. They need a solution that can analyze IAM policies and resource policies to detect unintended access paths to AWS resources such as S3 buckets, IAM roles, KMS keys, and SNS topics. Which solution should the team use to meet this requirement?

[ ] Use Amazon Inspector to detect over-permissive IAM policies and access paths across the environment

[CORRECT] Use AWS Identity and Access Management (IAM) Access Analyzer to evaluate resource-based and identity-based policies and identify resources shared outside the account or organization

[ ] Use IAM Access Advisor to get detailed access analysis of S3 bucket policies and determine which principals outside the organization have access

[ ] Use AWS Config to track configuration changes and infer resource-sharing behavior by analyzing compliance rules

Q41: An enterprise runs a critical Oracle database workload in its on-premises environment. The company now plans to replicate both existing records and continuous transactional changes to a managed Oracle environment in AWS. The target database will run on Amazon RDS for Oracle. Data transfer volume is expected to fluctuate throughout the day, and the team wants the solution to provision compute resources automatically based on actual workload requirements. Which solution will meet these requirements?

[ ] Use AWS Glue to extract data from the on-premises Oracle database and write the output to Amazon RDS for Oracle. Configure Glue to run on demand when changes are detected

[ ] Deploy the AWS DMS replication instance on Amazon EC2. Configure the instance with custom scripts that monitor CPU usage and resize the instance using EC2 Auto Scaling policies.

[ ] Use AWS Lambda to capture change data from the on-premises Oracle database. Trigger Lambda functions to write the updates to Amazon RDS for Oracle in real time.

[CORRECT] Configure an AWS DMS Serverless replication task to synchronize historical and ongoing changes between the on-premises Oracle database and Amazon RDS for Oracle

Q42: The engineering team at a retail company manages 3 Amazon EC2 instances that make read-heavy database requests to the Amazon RDS for the PostgreSQL database instance. As an AWS Certified Solutions Architect - Associate, you have been tasked to make the database instance resilient from a disaster recovery perspective. Which of the following features will help you in disaster recovery of the database? (Select two)

[CORRECT] Enable the automated backup feature of Amazon RDS in a multi-AZ deployment that creates backups across multiple Regions

[ ] Enable the automated backup feature of Amazon RDS in a multi-AZ deployment that creates backups in a single AWS Region

[ ] Use Amazon RDS Provisioned IOPS (SSD) Storage in place of General Purpose (SSD) Storage

[CORRECT] Use cross-Region Read Replicas

[ ] Use the database cloning feature of the Amazon RDS Database cluster

Q43: A DevOps team is tasked with enabling secure and temporary SSH access to Amazon EC2 instances for developers during deployments. The team wants to avoid distributing long-term SSH key pairs and instead prefers ephemeral access that can be audited and revoked immediately after the session ends. The team wants direct access via the AWS Management Console. What do you recommend?

[CORRECT] Use EC2 Instance Connect to inject a temporary public key and establish SSH access using the instance's public IP address

[ ] Use EC2 Instance Connect with Systems Manager Agent disabled, and connect via private IP using an internal proxy endpoint

[ ] Use an EC2 Instance Connect Endpoint to reach the instances even though they already have public IP addresses, because Instance Connect requires an endpoint for all SSH sessions

[ ] Use EC2 Instance Connect to inject a static SSH key and connect via the instance's private IP address directly from the internet

Q44: An online gaming company wants to block access to its application from specific countries; however, the company wants to allow its remote development team (from one of the blocked countries) to have access to the application. The application is deployed on Amazon EC2 instances running under an Application Load Balancer with AWS Web Application Firewall (AWS WAF). As a solutions architect, which of the following solutions can be combined to address the given use-case? (Select two)

[ ] Use Application Load Balancer IP set statement that specifies the IP addresses that you want to allow through

[ ] Create a deny rule for the blocked countries in the network access control list (network ACL) associated with each of the Amazon EC2 instances

[CORRECT] Use AWS WAF IP set statement that specifies the IP addresses that you want to allow through

[ ] Use Application Load Balancer geo match statement listing the countries that you want to block

[CORRECT] Use AWS WAF geo match statement listing the countries that you want to block

Q45: A digital design company has migrated its project archiving platform to AWS. The application runs on Amazon EC2 Linux instances in an Auto Scaling group that spans multiple Availability Zones. Designers upload and retrieve high-resolution image files from a shared file system, which is currently configured to use Amazon EFS Standard-IA. Metadata for these files is stored and indexed in an Amazon RDS for PostgreSQL database. The company's cloud engineering team has been asked to optimize storage costs for the image archive without compromising reliability. They are open to refactoring the application to use managed AWS services when necessary. Which solution offers the most cost-effective architecture?

[ ] Replace the EFS file system with Amazon FSx for NetApp ONTAP. Use volume tiering to move cold data to lower-cost capacity pool storage. Update the application to use the ONTAP mount path

[ ] Replace the EFS file system with Amazon FSx for Lustre. Mount the file system to EC2 instances and store project files there to reduce access latency and cost

[ ] Use AWS Backup to export all EFS files daily to an Amazon S3 bucket. Retain the EFS file system in Standard-IA class for occasional real-time access and route all archival queries to the S3 export

[CORRECT] Create an Amazon S3 bucket with Intelligent-Tiering enabled. Update the application to store and retrieve project files using the Amazon S3 API

Q46: A big data analytics company is using Amazon Kinesis Data Streams (KDS) to process IoT data from the field devices of an agricultural sciences company. Multiple consumer applications are using the incoming data streams and the engineers have noticed a performance lag for the data delivery speed between producers and consumers of the data streams. As a solutions architect, which of the following would you recommend for improving the performance for the given use-case?

[ ] Swap out Amazon Kinesis Data Streams with Amazon SQS FIFO queues

[CORRECT] Use Enhanced Fanout feature of Amazon Kinesis Data Streams

[ ] Swap out Amazon Kinesis Data Streams with Amazon SQS Standard queues

[ ] Swap out Amazon Kinesis Data Streams with Amazon Kinesis Data Firehose

Q47: A data analytics team at a global media firm is building a new analytics platform to process large volumes of both historical and real-time data. This data is stored in Amazon S3. The team wants to implement a serverless solution that allows them to query the data directly using SQL. Additionally, the solution must ensure that all data is encrypted at rest and automatically replicated to another AWS Region to support business continuity. Which solution will meet these requirements with the LEAST operational overhead?

[ ] Enable Cross-Region Replication (CRR) on the existing Amazon S3 bucket. Apply server-side encryption using AWS KMS multi-Region keys (SSE-KMS). Use Amazon Athena to run SQL queries on the replicated data

[CORRECT] Create an Amazon S3 bucket configured with server-side encryption using AWS KMS multi-Region keys (SSE-KMS). Enable cross-Region replication (CRR) on the source bucket. Use Amazon Athena to run SQL queries on the data

[ ] Enable Cross-Region Replication (CRR) on the existing Amazon S3 bucket. Apply server-side encryption using Amazon S3 managed keys (SSE-S3). Use Amazon Athena to run SQL queries on the replicated data

[ ] Create an Amazon S3 bucket configured with server-side encryption using Amazon S3 managed keys (SSE-S3). Enable cross-Region replication (CRR) on the source bucket. Use Amazon Redshift Spectrum to query the S3 data using SQL

Q48: A silicon valley based healthcare startup uses AWS Cloud for its IT infrastructure. The startup stores patient health records on Amazon Simple Storage Service (Amazon S3). The engineering team needs to implement an archival solution based on Amazon S3 Glacier to enforce regulatory and compliance controls on data access. As a solutions architect, which of the following solutions would you recommend?

[ ] Use Amazon S3 Glacier to store the sensitive archived data and then use an Amazon S3 lifecycle policy to enforce compliance controls

[ ] Use Amazon S3 Glacier vault to store the sensitive archived data and then use an Amazon S3 Access Control List to enforce compliance controls

[CORRECT] Use Amazon S3 Glacier vault to store the sensitive archived data and then use a vault lock policy to enforce compliance controls

[ ] Use Amazon S3 Glacier to store the sensitive archived data and then use an Amazon S3 Access Control List to enforce compliance controls

Q49: A company hosts a Microsoft SQL Server database on Amazon EC2 instances with attached Amazon EBS volumes. The operations team takes daily snapshots of these EBS volumes as backups. However, a recent incident occurred in which an automated script designed to clean up expired snapshots accidentally deleted all available snapshots, leading to potential data loss. The company wants to improve the backup strategy to avoid permanent data loss while still ensuring that old snapshots are eventually removed to optimize cost. A solutions architect needs to implement a mechanism that prevents immediate and irreversible deletion of snapshots. Which solution will best meet these requirements with the least development effort?

[CORRECT] Set up a 7-day EBS snapshot retention rule in Recycle Bin and apply the rule for all snapshots

[ ] Set up the IAM policy of the user to deny EBS snapshot deletion

[ ] Implement a Lambda-based backup automation workflow that archives snapshot metadata in DynamoDB and stores backups in Amazon S3 Glacier Deep Archive for long-term recovery

[ ] Enable AWS Backup Vault Lock on the backup vault and store EBS snapshots in that vault to enforce deletion protection

Q50: A retail company wants to establish encrypted network connectivity between its on-premises data center and AWS Cloud. The company wants to get the solution up and running in the fastest possible time and it should also support encryption in transit. As a solutions architect, which of the following solutions would you suggest to the company?

[ ] Use AWS Secrets Manager to establish encrypted network connectivity between the on-premises data center and AWS Cloud

[ ] Use AWS Data Sync to establish encrypted network connectivity between the on-premises data center and AWS Cloud

[ ] Use AWS Direct Connect to establish encrypted network connectivity between the on-premises data center and AWS Cloud

[CORRECT] Use AWS Site-to-Site VPN to establish encrypted network connectivity between the on-premises data center and AWS Cloud

Q51: An e-commerce company uses Amazon Simple Queue Service (Amazon SQS) queues to decouple their application architecture. The engineering team has observed message processing failures for some customer orders. As a solutions architect, which of the following solutions would you recommend for handling such message failures?

[ ] Use long polling to handle message processing failures

[CORRECT] Use a dead-letter queue to handle message processing failures

[ ] Use a temporary queue to handle message processing failures

[ ] Use short polling to handle message processing failures

Q52: You are a cloud architect at an IT company. The company has multiple enterprise customers that manage their own mobile applications that capture and send data to Amazon Kinesis Data Streams. They have been getting aProvisionedThroughputExceededExceptionexception. You have been contacted to help and upon analysis, you notice that messages are being sent one by one at a high rate. Which of the following options will help with the exception while keeping costs at a minimum?

[ ] Decrease the Stream retention duration

[CORRECT] Use batch messages

[ ] Increase the number of shards

[ ] Use Exponential Backoff

Q53: The engineering team at an e-commerce company uses an AWS Lambda function to write the order data into a single DB instance Amazon Aurora cluster. The team has noticed that many order- writes to its Aurora cluster are getting missed during peak load times. The diagnostics data has revealed that the database is experiencing high CPU and memory consumption during traffic spikes. The team also wants to enhance the availability of the Aurora DB. Which of the following steps would you combine to address the given scenario? (Select two)

[ ] Create a standby Aurora instance in another Availability Zone to improve the availability as the standby can serve as a failover target

[CORRECT] Handle all read operations for your application by connecting to the reader endpoint of the Amazon Aurora cluster so that Aurora can spread the load for read-only connections across the Aurora replica

[CORRECT] Create a replica Aurora instance in another Availability Zone to improve the availability as the replica can serve as a failover target

[ ] Increase the concurrency of the AWS Lambda function so that the order-writes do not get missed during traffic spikes

[ ] Use Amazon EC2 instances behind an Application Load Balancer to write the order data into Amazon Aurora cluster

Q54: An enterprise SaaS provider is currently operating a legacy web application hosted on a single Amazon EC2 instance within a public subnet. The same instance also hosts a MySQL database. DNS records for the application are configured through Amazon Route 53. As part of a modernization initiative, the company wants to rearchitect this application for high availability and scalability. In addition, the company wants to improve read performance on the database layer to handle increasing user traffic. Which combination of solutions will meet these requirements? (Select two)

[ ] Use an Auto Scaling group to deploy EC2 instances across multiple Availability Zones in two AWS Regions. Register the instances in a target group behind an Application Load Balancer to distribute web traffic evenly

[ ] Deploy an additional EC2 instance in a different AWS Region, and configure Amazon Route 53 with a failover routing policy to direct traffic to the secondary instance during primary Region outages

[CORRECT] Use an Auto Scaling group to deploy EC2 instances across multiple Availability Zones within a single Region. Register the instances in a target group behind an Application Load Balancer to distribute web traffic evenly

[ ] Use Amazon CloudFront with Lambda@Edge to serve dynamic content from EC2 instances located in different Regions

[CORRECT] Migrate the existing MySQL database to an Amazon Aurora MySQL cluster. Deploy the primary DB instance and one or more read replicas in different Availability Zones

Q55: The data engineering team at an e-commerce company has set up a workflow to ingest the clickstream data into the raw zone of the Amazon S3 data lake. The team wants to run some SQL based data sanity checks on the raw zone of the data lake. What AWS services would you recommend for this use-case such that the solution is cost-effective and easy to maintain?

[ ] Load the incremental raw zone data into Amazon RDS on an hourly basis and run the SQL based sanity checks

[CORRECT] Use Amazon Athena to run SQL based analytics against Amazon S3 data

[ ] Load the incremental raw zone data into Amazon Redshift on an hourly basis and run the SQL based sanity checks

[ ] Load the incremental raw zone data into an Amazon EMR based Spark Cluster on an hourly basis and use SparkSQL to run the SQL based sanity checks

Q56: A media streaming company expects a major increase in user activity during the launch of a highly anticipated live event. The streaming platform is deployed on AWS and uses Amazon EC2 instances for the application layer and Amazon RDS for persistent storage. The operations team needs to proactively monitor system performance to ensure a smooth user experience during the event. Their monitoring setup must provide data visibility with intervals of no more than 2 minutes, and the team prefers a solution that is quick to implement and low-maintenance. Which solution should the team implement?

[ ] Install the CloudWatch agent on all EC2 instances. Configure the agent to collect high-resolution custom metrics and stream them to CloudWatch Logs for analysis via Amazon Athena

[ ] Use Amazon EventBridge to collect EC2 state changes and publish them to Amazon SNS. Subscribe a monitoring dashboard to the SNS topic to visualize metrics

[ ] Stream EC2 system logs to an Amazon OpenSearch Service domain for real-time indexing and visualization. Use OpenSearch Dashboards to monitor CPU and memory metrics

[CORRECT] Enable detailed monitoring on all EC2 instances and use Amazon CloudWatch metrics to track performance

Q57: A leading media company wants to do an accelerated online migration of hundreds of terabytes of files from their on-premises data center to Amazon S3 and then establish a mechanism to access the migrated data for ongoing updates from the on-premises applications. As a solutions architect, which of the following would you select as the MOST performant solution for the given use-case?

[CORRECT] Use AWS DataSync to migrate existing data to Amazon S3 and then use File Gateway to retain access to the migrated data for ongoing updates from the on-premises applications

[ ] Use File Gateway configuration of AWS Storage Gateway to migrate data to Amazon S3 and then use Amazon S3 Transfer Acceleration (Amazon S3TA) for ongoing updates from the on-premises applications

[ ] Use AWS DataSync to migrate existing data to Amazon S3 as well as access the Amazon S3 data for ongoing updates

[ ] Use Amazon S3 Transfer Acceleration (Amazon S3TA) to migrate existing data to Amazon S3 and then use AWS DataSync for ongoing updates from the on-premises applications

Q58: A media company wants to get out of the business of owning and maintaining its own IT infrastructure. As part of this digital transformation, the media company wants to archive about 5 petabytes of data in its on-premises data center to durable long term storage. As a solutions architect, what is your recommendation to migrate this data in the MOST cost-optimal way?

[CORRECT] Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized devices. Copy the AWS Snowball Edge data into Amazon S3 and create a lifecycle policy to transition the data into Amazon S3 Glacier

[ ] Setup AWS direct connect between the on-premises data center and AWS Cloud. Use this connection to transfer the data into Amazon S3 Glacier

[ ] Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized devices. Copy the AWS Snowball Edge data into Amazon S3 Glacier

[ ] Setup AWS Site-to-Site VPN connection between the on-premises data center and AWS Cloud. Use this connection to transfer the data into Amazon S3 Glacier

Q59: A streaming service provider collects user experience feedback through embedded feedback forms in their mobile and web apps. Feedback submissions frequently spike to thousands per hour during content launches or service outages. Currently, the feedback is sent via email to the operations team for manual review. The company now wants to automate feedback collection and sentiment analysis so that insights can be generated quickly and stored for a full year for trend analysis. Which solution provides the most scalable and automated approach to meet these requirements?

[CORRECT] Design a RESTful API with Amazon API Gateway that forwards incoming feedback data to an Amazon SQS queue. Set up an AWS Lambda function to process the queue messages, analyze sentiment using Amazon Comprehend, and store results in a DynamoDB table with a 365-day TTL configured on each item

[ ] Build a web service on Amazon EC2 that receives feedback data and stores each record in a DynamoDB table. Use the EC2 application to invoke Amazon Comprehend for sentiment detection and write results to a second table. Apply a TTL of 365 days to each table

[ ] Use Amazon EventBridge to capture feedback events and forward them to an AWS Step Functions workflow. The workflow invokes Lambda functions for validation, calls Amazon Transcribe to convert the text to audio for archival, and stores the results in an Amazon RDS database. Configure a lifecycle policy to remove records after 12 months

[ ] Route all feedback submissions through Amazon Kinesis Data Streams. Use an AWS Lambda consumer to batch process incoming records, invoke Amazon Translate to detect language and convert input to English, and save the processed content in an Amazon OpenSearch Service index. Configure OpenSearch Index State Management (ISM) policies to delete documents after 12 months

Q60: A global media company uses a fleet of Amazon EC2 instances (behind an Application Load Balancer) to power its video streaming application. To improve the performance of the application, the engineering team has also created an Amazon CloudFront distribution with the Application Load Balancer as the custom origin. The security team at the company has noticed a spike in the number and types of SQL injection and cross-site scripting attack vectors on the application. As a solutions architect, which of the following solutions would you recommend as the MOST effective in countering these malicious attacks?

[ ] Use Amazon Route 53 with Amazon CloudFront distribution

[ ] Use AWS Firewall Manager with CloudFront distribution

[CORRECT] Use AWS Web Application Firewall (AWS WAF) with Amazon CloudFront distribution

[ ] Use AWS Security Hub with Amazon CloudFront distribution

Q61: A financial analytics firm runs performance-intensive modeling software on Amazon EC2 instances backed by Amazon EBS volumes. The production data resides on EBS volumes attached to EC2 instances in the same AWS Region where the testing environment is hosted. To maintain data integrity, any changes made during testing must not affect production data. The development team needs to frequently create clones of this production data for simulations. The modeling software requires high and consistent I/O performance, and the firm wants to minimize the time required to provision test data. Which solution should a solutions architect recommend to meet these requirements?

[CORRECT] Take snapshots of the production EBS volumes. Enable EBS fast snapshot restore on the snapshots. Create new EBS volumes from the snapshots and attach them to EC2 instances in the test environment

[ ] Use Amazon EBS io2 volumes with Multi-Attach enabled. Attach the same production EBS volumes to both the production and test EC2 instances simultaneously to avoid cloning delays and ensure high IOPS performance

[ ] Create new EBS volumes in the test environment and use AWS Backup to perform a backup job of the production volumes. Restore the backup directly to the test EBS volumes to begin simulations

[ ] Create Amazon EBS-backed Amazon Machine Images (AMIs) from the production EC2 instances. Launch new EC2 instances in the test environment from the AMIs. Use Amazon EC2 instance store volumes for temporary simulation data

Q62: A multinational logistics company operates its shipment tracking platform from Amazon EC2 instances deployed in the AWS us-west-2 Region. The platform exposes a set of APIs over HTTPS, which are used by logistics partners and customers around the world to retrieve real-time tracking data. The company has observed that users from Europe and Asia experience latency issues and inconsistent API response times when accessing the service. As a cloud architect, you have been tasked to propose the most cost-effective solution to improve performance for these international users without migrating the application. Which solution should you recommend?

[CORRECT] Set up AWS Global Accelerator with listeners configured for HTTPS. Create endpoint groups for Europe and Asia and add the existing us-west-2 EC2 endpoint to these groups

[ ] Deploy Amazon API Gateway in multiple AWS Regions and synchronize the API definitions. Use AWS Lambda as a proxy to forward requests to the EC2-hosted API in us-west-2

[ ] Use Amazon Route 53 latency-based routing to direct user requests to a copy of the EC2 API deployed in each major geographic Region

[ ] Deploy an Amazon CloudFront distribution in front of the API endpoint and apply the CachingOptimized managed policy to enhance caching behavior and improve content delivery efficiency

Q63: A media company operates a web application that enables users to upload photos. These uploads are stored in an Amazon S3 bucket located in the eu-west-2 Region. To enhance performance and provide secure access under a custom domain name, the company wants to integrate Amazon CloudFront for uploads to the S3 bucket. The architecture must support secure HTTPS connections using a custom domain, and the upload process must ensure optimal speed and security. Which combination of actions will fulfill these requirements? (Select two)

[ ] Request a public certificate from AWS Certificate Manager (ACM) in the eu-west-2 Region and associate it with the CloudFront distribution

[ ] Create a CloudFront distribution with an S3 static website endpoint as the origin and enable upload operations

[ ] Set up a custom origin request policy in CloudFront that includes all viewer headers and query strings. Enable S3 Object Ownership to allow CloudFront to assume control of uploaded files via a signed URL

[CORRECT] Set up Amazon S3 to accept uploads from CloudFront by enabling origin access control (OAC)

[CORRECT] Request a public certificate from AWS Certificate Manager (ACM) in the us-east-1 Region and associate it with the CloudFront distribution

Q64: A digital media company runs its content rendering service on Amazon EC2 instances that are registered with an Application Load Balancer (ALB) using IP-based target groups. The company relies on AWS Systems Manager to manage and patch these instances regularly. According to new compliance requirements, EC2 instances must be safely removed from production traffic during patching to prevent user disruption and maintain application integrity. However, during the most recent patch cycle, the operations team noticed application failures and API timeouts, even though patching succeeded on the instances. You are asked to suggest a reliable and scalable way to ensure safe patching while preserving service availability. Which solution will best meet the new compliance and operational requirements? (Select two)

[CORRECT] Configure Systems Manager Maintenance Windows to coordinate patching and instance removal from the ALB during the defined window

[ ] Modify the load balancer configuration to attach EC2 instances using instance ID-based target groups instead of IP-based targets, allowing Systems Manager to directly communicate with instance metadata

[CORRECT] Use AWS Systems Manager Automation with the AWSEC2-PatchLoadBalancerInstance document to manage patching

[ ] Configure a custom Lambda function triggered by an Amazon EventBridge rule that disables the EC2 instance's network interface during the patching window and re-enables it after patching completes

[ ] Use Amazon CloudWatch Logs Insights to monitor patching success and then manually adjust ALB target group registrations before and after each patch window

Q65: The engineering team at a weather tracking company wants to enhance the performance of its relational database and is looking for a caching solution that supports geospatial data. As a solutions architect, which of the following solutions will you suggest?

[ ] Use Amazon DynamoDB Accelerator (DAX)

[ ] Use Amazon ElastiCache for Memcached

[ ] Use AWS Global Accelerator

[CORRECT] Use Amazon ElastiCache for Redis