Exam Questions Export

Q1: A retail company wants to share sensitive accounting data that is stored in an Amazon RDS database instance with an external auditor. The auditor has its own AWS account and needs its own copy of the database. Which of the following would you recommend to securely share the database with the auditor?

[ ] Set up a read replica of the database and configure IAM standard database authentication to grant the auditor access

[ ] Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket

[ ] Create a snapshot of the database in Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket

[CORRECT] Create an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key

Q2: You are establishing a monitoring solution for desktop systems, that will be sending telemetry data into AWS every 1 minute. Data for each system must be processed in order, independently, and you would like to scale the number of consumers to be possibly equal to the number of desktop systems that are being monitored. What do you recommend?

[ ] Use an Amazon Simple Queue Service (Amazon SQS) standard queue, and send the telemetry data as is

[CORRECT] Use an Amazon Simple Queue Service (Amazon SQS) FIFO (First-In-First-Out) queue, and make sure the telemetry data is sent with a Group ID attribute representing the value of the Desktop ID

[ ] Use an Amazon Simple Queue Service (Amazon SQS) FIFO (First-In-First-Out) queue, and send the telemetry data as is

[ ] Use an Amazon Kinesis Data Stream, and send the telemetry data with a Partition ID that uses the value of the Desktop ID

Q3: "An enterprise organization is expanding its cloud footprint and needs to centralize its security event data from various AWS accounts and services. The goal is to evaluate security posture across all environments and improve threat detection and response — without requiring significant custom code or manual integration. Which solution will fulfill these needs with the least development effort?

[CORRECT] Use Amazon Security Lake to create a centralized data lake that automatically collects security-related logs and events from AWS services and third-party sources. Store the data in an Amazon S3 bucket managed by Security Lake

[ ] Use Amazon Athena with predefined SQL queries to scan security logs stored in multiple S3 buckets. Visualize the findings by exporting results to an Amazon QuickSight dashboard

[ ] Deploy a custom Lambda function to aggregate security logs from multiple AWS accounts. Format the data into CSV files and upload them to a central S3 bucket for analysis

[ ] Set up a data lake using AWS Lake Formation to collect and organize security event logs. Use AWS Glue to perform ETL operations and standardize the log formats for centralized analysis

Q4: A manufacturing analytics company has a large collection of automated scripts that perform data cleanup, validation, and system integration tasks. These scripts are currently run by a local Linux cron scheduler and have an execution time of up to 30 minutes. The company wants to migrate these scripts to AWS without significant changes, and would prefer a containerized, serverless architecture that automatically scales and can respond to event-based triggers in the future. The solution must minimize infrastructure management. Which solution will best meet these requirements with minimal refactoring and operational overhead?

[ ] Package the scripts into a container image. Deploy the image to AWS Batch with a managed compute environment on Amazon EC2. Define scheduling policies in AWS Batch to trigger jobs according to cron expressions

[CORRECT] Package the scripts into a container image. Use Amazon EventBridge Scheduler to define cron-based recurring schedules. Configure EventBridge Scheduler to invoke AWS Fargate tasks using Amazon ECS

[ ] Create a container image for each script. Use AWS Step Functions to define a workflow for all scheduled tasks. Use a Wait state to delay execution and run tasks using Step Functions' RunTask integration with ECS Fargate

[ ] Convert each script into a Lambda function and package it in a zip archive. Use Amazon EventBridge Scheduler to run the functions on a fixed schedule. Use Amazon S3 to store function outputs and logs

Q5: The engineering team at a logistics company has noticed that the Auto Scaling group (ASG) is not terminating an unhealthy Amazon EC2 instance. As a Solutions Architect, which of the following options would you suggest to troubleshoot the issue? (Select three)

[ ] A user might have updated the configuration of the Auto Scaling group (ASG) and increased the minimum number of instances forcing ASG to keep all instances alive

[CORRECT] The health check grace period for the instance has not expired

[ ] The Amazon EC2 instance could be a spot instance type, which cannot be terminated by the Auto Scaling group (ASG)

[CORRECT] The instance has failed the Elastic Load Balancing (ELB) health check status

[ ] A custom health check might have failed. The Auto Scaling group (ASG) does not terminate instances that are set unhealthy by custom checks

[CORRECT] The instance maybe in Impaired status

Q6: A silicon valley based startup has a content management application with the web-tier running on Amazon EC2 instances and the database tier running on Amazon Aurora. Currently, the entire infrastructure is located inus-east-1region. The startup has 90% of its customers in the US and Europe. The engineering team is getting reports of deteriorated application performance from customers in Europe with high application load time. As a solutions architect, which of the following would you recommend addressing these performance issues? (Select two)

[ ] Setup another fleet of Amazon EC2 instances for the web tier in the eu-west-1 region. Enable geolocation routing policy in Amazon Route 53

[ ] Create Amazon Aurora Multi-AZ standby instance in the eu-west-1 region

[CORRECT] Create Amazon Aurora read replicas in the eu-west-1 region

[ ] Setup another fleet of Amazon EC2 instances for the web tier in the eu-west-1 region. Enable failover routing policy in Amazon Route 53

[CORRECT] Setup another fleet of Amazon EC2 instances for the web tier in the eu-west-1 region. Enable latency routing policy in Amazon Route 53

Q7: Which of the following IAM policies provides read-only access to the Amazon S3 bucketmybucketand its content?

[CORRECT] { "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":["s3:ListBucket"], "Resource":"arn:aws:s3:::mybucket" }, { "Effect":"Allow", "Action":["s3:GetObject"], "Resource":"arn:aws:s3:::mybucket/*" }] }

[ ] { "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":["s3:ListBucket"], "Resource":"arn:aws:s3:::mybucket/*" }, { "Effect":"Allow", "Action":["s3:GetObject"], "Resource":"arn:aws:s3:::mybucket" }] }

[ ] { "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":["s3:ListBucket", "s3:GetObject"], "Resource":"arn:aws:s3:::mybucket/*" }] }

[ ] { "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":["s3:ListBucket", "s3:GetObject"], "Resource":"arn:aws:s3:::mybucket" }] }

Q8: A retail company wants to rollout and test a blue-green deployment for its global application in the next 48 hours. Most of the customers use mobile phones which are prone to Domain Name System (DNS) caching. The company has only two days left for the annual Thanksgiving sale to commence. As a Solutions Architect, which of the following options would you recommend to test the deployment on as many users as possible in the given time frame?

[ ] Use Amazon Route 53 weighted routing to spread traffic across different deployments

[ ] Use AWS CodeDeploy deployment options to choose the right deployment

[ ] Use Elastic Load Balancing (ELB) to distribute traffic across deployments

[CORRECT] Use AWS Global Accelerator to distribute a portion of traffic to a particular deployment

Q9: Your company has a monthly big data workload, running for about 2 hours, which can be efficiently distributed across multiple servers of various sizes, with a variable number of CPUs. The solution for the workload should be able to withstand server failures. Which is the MOST cost-optimal solution for this workload?

[ ] Run the workload on Reserved Instances (RI)

[CORRECT] Run the workload on a Spot Fleet

[ ] Run the workload on Spot Instances

[ ] Run the workload on Dedicated Hosts

Q10: A startup has just developed a video backup service hosted on a fleet of Amazon EC2 instances. The Amazon EC2 instances are behind an Application Load Balancer and the instances are using Amazon Elastic Block Store (Amazon EBS) Volumes for storage. The service provides authenticated users the ability to upload videos that are then saved on the EBS volume attached to a given instance. On the first day of the beta launch, users start complaining that they can see only some of the videos in their uploaded videos backup. Every time the users log into the website, they claim to see a different subset of their uploaded videos. Which of the following is the MOST optimal solution to make sure that users can view all the uploaded videos? (Select two)

[CORRECT] Write a one time job to copy the videos from all Amazon EBS volumes to Amazon S3 and then modify the application to use Amazon S3 standard for storing the videos

[ ] Write a one time job to copy the videos from all Amazon EBS volumes to Amazon RDS and then modify the application to use Amazon RDS for storing the videos

[CORRECT] Mount Amazon Elastic File System (Amazon EFS) on all Amazon EC2 instances. Write a one time job to copy the videos from all Amazon EBS volumes to Amazon EFS. Modify the application to use Amazon EFS for storing the videos

[ ] Write a one time job to copy the videos from all Amazon EBS volumes to Amazon DynamoDB and then modify the application to use Amazon DynamoDB for storing the videos

[ ] Write a one time job to copy the videos from all Amazon EBS volumes to Amazon S3 Glacier Deep Archive and then modify the application to use Amazon S3 Glacier Deep Archive for storing the videos

Q11: A Machine Learning research group uses a proprietary computer vision application hosted on an Amazon EC2 instance. Every time the instance needs to be stopped and started again, the application takes about 3 minutes to start as some auxiliary software programs need to be executed so that the application can function. The research group would like to minimize the application boostrap time whenever the system needs to be stopped and then started at a later point in time. As a solutions architect, which of the following solutions would you recommend for this use-case?

[ ] Use Amazon EC2 Meta-Data

[ ] Create an Amazon Machine Image (AMI) and launch your Amazon EC2 instances from that

[ ] Use Amazon EC2 User-Data

[CORRECT] Use Amazon EC2 Instance Hibernate

Q12: An enterprise is building a secure business intelligence API using Amazon API Gateway to serve internal users with confidential analytics data. The API must be accessible only from a set of trusted IP addresses that are part of the organization's internal network ranges. No external IP traffic should be able to invoke the API. A solutions architect must design this access control mechanism with the least operational complexity. What should the architect do to meet these requirements?

[CORRECT] Create a resource policy for the API Gateway API that explicitly denies access to all IP addresses except those listed in an allow list

[ ] Deploy the API Gateway resource to an on-premises server using AWS Outposts. Apply host-based firewall rules to filter allowed IPs

[ ] Modify the security group that is attached to API Gateway to allow only traffic from specific IP addresses

[ ] Deploy the API Gateway as a regional API in a public subnet and associate the subnet with a security group that permits inbound traffic only from trusted IP ranges

Q13: A financial services company wants to store confidential data in Amazon S3 and it needs to meet the following data security and compliance norms: Which is the MOST operationally efficient solution?

[CORRECT] Server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) with automatic key rotation

[ ] Server-side encryption (SSE-S3) with automatic key rotation

[ ] Server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) with manual key rotation

[ ] Server-side encryption with customer-provided keys (SSE-C) with automatic key rotation

Q14: An application is currently hosted on four Amazon EC2 instances (behind Application Load Balancer) deployed in a single Availability Zone (AZ). To maintain an acceptable level of end-user experience, the application needs at least 4 instances to be always available. As a solutions architect, which of the following would you recommend so that the application achieves high availability with MINIMUM cost?

[ ] Deploy the instances in two Availability Zones (AZs). Launch four instances in each Availability Zone (AZ)

[ ] Deploy the instances in two Availability Zones (AZs). Launch two instances in each Availability Zone (AZ)

[CORRECT] Deploy the instances in three Availability Zones (AZs). Launch two instances in each Availability Zone (AZ)

[ ] Deploy the instances in one Availability Zones. Launch two instances in the Availability Zone (AZ)

Q15: Amazon EC2 Auto Scaling needs to terminate an instance from Availability Zone (AZ)us-east-1aas it has the most number of instances amongst the Availability Zone (AZs) being used currently. There are 4 instances in the Availability Zone (AZ)us-east-1alike so: Instance A has the oldest launch template, Instance B has the oldest launch configuration, Instance C has the newest launch configuration and Instance D is closest to the next billing hour. Which of the following instances would be terminated per the default termination policy?

[ ] Instance C

[ ] Instance A

[CORRECT] Instance B

[ ] Instance D

Q16: A manufacturing company receives unreliable service from its data center provider because the company is located in an area prone to natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failover environment on AWS in case the on-premises data center fails. The company runs web servers that connect to external vendors. The data available on AWS and on-premises must be uniform. Which of the following solutions would have the LEAST amount of downtime?

[ ] Set up a Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to provision Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3

[CORRECT] Set up a Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3

[ ] Set up a Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer

[ ] Set up a Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center

Q17: You have multiple AWS accounts within a single AWS Region managed by AWS Organizations and you would like to ensure all Amazon EC2 instances in all these accounts can communicate privately. Which of the following solutions provides the capability at the CHEAPEST cost?

[CORRECT] Create a virtual private cloud (VPC) in an account and share one or more of its subnets with the other accounts using Resource Access Manager

[ ] Create a VPC peering connection between all virtual private cloud (VPCs)

[ ] Create a Private Link between all the Amazon EC2 instances

[ ] Create an AWS Transit Gateway and link all the virtual private cloud (VPCs) in all the accounts together

Q18: An IT company has built a solution wherein an Amazon Redshift cluster writes data to an Amazon S3 bucket belonging to a different AWS account. However, it is found that the files created in the Amazon S3 bucket using the UNLOAD command from the Amazon Redshift cluster are not even accessible to the Amazon S3 bucket owner. What could be the reason for this denial of permission for the bucket owner?

[CORRECT] By default, an Amazon S3 object is owned by the AWS account that uploaded it. So the Amazon S3 bucket owner will not implicitly have access to the objects written by the Amazon Redshift cluster

[ ] When two different AWS accounts are accessing an Amazon S3 bucket, both the accounts must share the bucket policies. An erroneous policy can lead to such permission failures

[ ] The owner of an Amazon S3 bucket has implicit access to all objects in his bucket. Permissions are set on objects after they are completely copied to the target location. Since the owner is unable to access the uploaded files, the write operation may be still in progress

[ ] When objects are uploaded to Amazon S3 bucket from a different AWS account, the S3 bucket owner will get implicit permissions to access these objects. This issue seems to be due to an upload error that can be fixed by providing manual access from AWS console

Q19: An HTTP application is deployed on an Auto Scaling Group, is accessible from an Application Load Balancer (ALB) that provides HTTPS termination, and accesses a PostgreSQL database managed by Amazon RDS. How should you configure the security groups? (Select three)

[CORRECT] The security group of the Application Load Balancer should have an inbound rule from anywhere on port 443

[ ] The security group of the Application Load Balancer should have an inbound rule from anywhere on port 80

[ ] The security group of Amazon RDS should have an inbound rule from the security group of the Amazon EC2 instances in the Auto Scaling group on port 80

[CORRECT] The security group of the Amazon EC2 instances should have an inbound rule from the security group of the Application Load Balancer on port 80

[CORRECT] The security group of Amazon RDS should have an inbound rule from the security group of the Amazon EC2 instances in the Auto Scaling group on port 5432

[ ] The security group of the Amazon EC2 instances should have an inbound rule from the security group of the Amazon RDS database on port 5432

Q20: A systems administrator has created a private hosted zone and associated it with a Virtual Private Cloud (VPC). However, the Domain Name System (DNS) queries for the private hosted zone remain unresolved. As a Solutions Architect, can you identify the Amazon Virtual Private Cloud (Amazon VPC) options to be configured in order to get the private hosted zone to work?

[ ] Fix the Name server (NS) record and Start Of Authority (SOA) records that may have been created with wrong configurations

[ ] Remove any overlapping namespaces for the private and public hosted zones

[ ] Fix conflicts between your private hosted zone and any Resolver rule that routes traffic to your network for the same domain name, as it results in ambiguity over the route to be taken

[CORRECT] Enable DNS hostnames and DNS resolution for private hosted zones

Q21: An enterprise uses a centralized Amazon S3 bucket to store logs and reports generated by multiple analytics services. Each service writes to and reads from a dedicated prefix (folder path) in the bucket. The company wants to enforce fine-grained access control so that each service can access only its own prefix, without being able to see or modify other services' data. The solution must support scalable and maintainable permissions management with minimal operational overhead. Which approach will best meet these requirements?

[ ] Create a single S3 bucket policy that lists all object ARNs under each prefix and grants permissions accordingly. Use resource-level permissions to restrict access to individual services

[CORRECT] Configure individual S3 access points for each analytics service. Attach access point policies that restrict access to only the relevant prefix in the S3 bucket

[ ] Deploy Amazon Macie to classify the objects in the bucket by prefix and apply automated object-level access policies to each object based on service tags

[ ] Create separate IAM users for each service. Manually assign inline IAM policies to grant read/write permissions to the S3 bucket. Reference specific object names in the policy for each user

Q22: Upon a security review of your AWS account, an AWS consultant has found that a few Amazon RDS databases are unencrypted. As a Solutions Architect, what steps must be taken to encrypt the Amazon RDS databases?

[ ] Enable encryption on the Amazon RDS database using the AWS Console

[ ] Create a Read Replica of the database, and encrypt the read replica. Promote the read replica as a standalone database, and terminate the previous database

[ ] Enable Multi-AZ for the database, and make sure the standby instance is encrypted. Stop the main database to that the standby database kicks in, then disable Multi-AZ

[CORRECT] Take a snapshot of the database, copy it as an encrypted snapshot, and restore a database from the encrypted snapshot. Terminate the previous database

Q23: An IT company wants to optimize the costs incurred on its fleet of 100 Amazon EC2 instances for the next year. Based on historical analyses, the engineering team observed that 70 of these instances handle the compute services of its flagship application and need to be always available. The other 30 instances are used to handle batch jobs that can afford a delay in processing. As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution?

[ ] Purchase 70 on-demand instances and 30 reserved instances

[CORRECT] Purchase 70 reserved instances (RIs) and 30 spot instances

[ ] Purchase 70 reserved instances and 30 on-demand instances

[ ] Purchase 70 on-demand instances and 30 spot instances

Q24: A media company is migrating its flagship application from its on-premises data center to AWS for improving the application's read-scaling capability as well as its availability. The existing architecture leverages a Microsoft SQL Server database that sees a heavy read load. The engineering team does a full copy of the production database at the start of the business day to populate a dev database. During this period, application users face high latency leading to a bad user experience. The company is looking at alternate database options and migrating database engines if required. What would you suggest?

[CORRECT] Leverage Amazon Aurora MySQL with Multi-AZ Aurora Replicas and create the dev database by restoring from the automated backups of Amazon Aurora

[ ] Leverage Amazon Aurora MySQL with Multi-AZ Aurora Replicas and restore the dev database via mysqldump

[ ] Leverage Amazon RDS for SQL server with a Multi-AZ deployment and read replicas. Use the read replica as the dev database

[ ] Leverage Amazon RDS for MySQL with a Multi-AZ deployment and use the standby instance as the dev database

Q25: A media production studio is building a content rendering and editing platform on AWS. The editing workstations and rendering tools require access to shared files over the SMB (Server Message Block) protocol. The studio wants a managed storage solution that is simple to set up, integrates easily with SMB clients, and minimizes ongoing operational tasks. Which solution will best meet the requirements with the LEAST administrative overhead?

[ ] Set up an AWS Storage Gateway Volume Gateway in cached volume mode. Attach the volume as an iSCSI device to the application server and configure a file system with SMB sharing enabled

[ ] Launch an Amazon EC2 Windows instance and manually configure a Windows file share. Use this instance to serve SMB access to application clients

[ ] Use Amazon S3 with Transfer Acceleration enabled. Configure the application to upload and download files over HTTPS using signed URLs

[CORRECT] Provision an Amazon FSx for Windows File Server file system. Mount the file system using the SMB protocol on the media servers

Q26: An IT company is working on a client project to build a Supply Chain Management application. The web-tier of the application runs on an Amazon EC2 instance and the database tier is on Amazon RDS MySQL. For beta testing, all the resources are currently deployed in a single Availability Zone (AZ). The development team wants to improve application availability before the go-live. Given that all end users of the web application would be located in the US, which of the following would be the MOST resource-efficient solution?

[ ] Deploy the web-tier Amazon EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration

[ ] Deploy the web-tier Amazon EC2 instances in two Availability Zones (AZs), behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in read replica configuration

[CORRECT] Deploy the web-tier Amazon EC2 instances in two Availability Zones (AZs), behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration

[ ] Deploy the web-tier Amazon EC2 instances in two regions, behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration

Q27: A social photo-sharing web application is hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in Amazon Simple Storage Service (Amazon S3) and the leaderboard data is maintained in Amazon DynamoDB. The Amazon EC2 instances need to access both Amazon S3 and Amazon DynamoDB for these features. As a solutions architect, which of the following solutions would you recommend as the MOST secure option?

[ ] Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the Amazon EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to Amazon S3 and Amazon DynamoDB

[ ] Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the Amazon EC2 instances. Amazon EC2 instances can use these credentials to access Amazon S3 and Amazon DynamoDB

[ ] Configure AWS CLI on the Amazon EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access Amazon S3 and Amazon DynamoDB via AWS CLI

[CORRECT] Attach the appropriate IAM role to the Amazon EC2 instance profile so that the instance can access Amazon S3 and Amazon DynamoDB

Q28: A company has recently launched a new mobile gaming application that the users are adopting rapidly. The company uses Amazon RDS MySQL as the database. The engineering team wants an urgent solution to this issue where the rapidly increasing workload might exceed the available database storage. As a solutions architect, which of the following solutions would you recommend so that it requires minimum development and systems administration effort to address this requirement?

[CORRECT] Enable storage auto-scaling for Amazon RDS MySQL

[ ] Create read replica for Amazon RDS MySQL

[ ] Migrate Amazon RDS MySQL database to Amazon DynamoDB which automatically allocates storage space when required

[ ] Migrate RDS MySQL database to Amazon Aurora which offers storage auto-scaling

Q29: A social media application is hosted on an Amazon EC2 fleet running behind an Application Load Balancer. The application traffic is fronted by an Amazon CloudFront distribution. The engineering team wants to decouple the user authentication process for the application, so that the application servers can just focus on the business logic. As a Solutions Architect, which of the following solutions would you recommend to the development team so that it requires minimal development effort?

[ ] Use Amazon Cognito Authentication via Cognito Identity Pools for your Application Load Balancer

[ ] Use Amazon Cognito Authentication via Cognito User Pools for your Amazon CloudFront distribution

[ ] Use Amazon Cognito Authentication via Cognito Identity Pools for your Amazon CloudFront distribution

[CORRECT] Use Amazon Cognito Authentication via Cognito User Pools for your Application Load Balancer

Q30: An IT company has an Access Control Management (ACM) application that uses Amazon RDS for MySQL but is running into performance issues despite using Read Replicas. The company has hired you as a solutions architect to address these performance-related challenges without moving away from the underlying relational database schema. The company has branch offices across the world, and it needs the solution to work on a global scale. Which of the following will you recommend as the MOST cost-effective and high-performance solution?

[ ] Spin up Amazon EC2 instances in each AWS region, install MySQL databases and migrate the existing data into these new databases

[ ] Spin up a Amazon Redshift cluster in each AWS region. Migrate the existing data into Redshift clusters

[CORRECT] Use Amazon Aurora Global Database to enable fast local reads with low latency in each region

[ ] Use Amazon DynamoDB Global Tables to provide fast, local, read and write performance in each region

Q31: A multinational logistics company is migrating its core systems to AWS. As part of this migration, the company has built an Amazon S3–based data lake to ingest and analyze supply chain data from external carriers and vendors. While some vendors have adopted the company's modern REST-based APIs for S3 uploads, others operate legacy systems that rely exclusively on SFTP for file transfers. These vendors are unable or unwilling to modify their workflows to support S3 APIs. The company wants to provide these vendors with an SFTP-compatible solution that allows direct uploads to Amazon S3, and must use fully managed AWS services to avoid managing any infrastructure. It must also support identity federation so that internal teams can map vendor access securely to specific S3 buckets or prefixes. Which combination of options will provide a scalable and low-maintenance solution for this use case? (Select two)

[CORRECT] Deploy a fully managed AWS Transfer Family endpoint with SFTP enabled. Configure it to store uploaded files directly in an Amazon S3 bucket. Set up IAM roles mapped to each vendor for secure bucket or prefix access

[CORRECT] Configure Amazon S3 bucket policies to use IAM role-based access control for each vendor. Combine this with Transfer Family identity provider integration using Amazon Cognito or a custom identity provider for fine-grained permissions

[ ] Use Amazon AppFlow to extract data from the legacy vendor systems and transform it into S3-compliant uploads. Schedule batch sync jobs to trigger every hour and send logs to CloudWatch for audit purposes

[ ] Use AWS Transfer Family with SFTP for file uploads. Integrate the SFTP access control with Amazon Route 53 private hosted zones to create vendor-specific upload subdomains pointing to the SFTP endpoint

[ ] Set up an Amazon EC2 instance with a custom SFTP server using OpenSSH. Configure cron jobs to upload received files to S3. Use Amazon CloudWatch to monitor EC2 health and disk usage

Q32: The engineering manager for a content management application wants to set up Amazon RDS read replicas to provide enhanced performance and read scalability. The manager wants to understand the data transfer charges while setting up Amazon RDS read replicas. Which of the following would you identify as correct regarding the data transfer charges for Amazon RDS read replicas?

[CORRECT] There are data transfer charges for replicating data across AWS Regions

[ ] There are data transfer charges for replicating data within the same Availability Zone (AZ)

[ ] There are no data transfer charges for replicating data across AWS Regions

[ ] There are data transfer charges for replicating data within the same AWS Region

Q33: You have a team of developers in your company, and you would like to ensure they can quickly experiment with AWS Managed Policies by attaching them to their accounts, but you would like to prevent them from doing an escalation of privileges, by granting themselves theAdministratorAccessmanaged policy. How should you proceed?

[CORRECT] For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves

[ ] Attach an IAM policy to your developers, that prevents them from attaching the AdministratorAccess policy

[ ] Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves

[ ] Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the AdministratorAccess policy

Q34: An engineering team wants to examine the feasibility of theuser datafeature of Amazon EC2 for an upcoming project. Which of the following are true about the Amazon EC2 user data configuration? (Select two)

[ ] By default, scripts entered as user data do not have root user privileges for executing

[ ] When an instance is running, you can update user data by using root user credentials

[ ] By default, user data is executed every time an Amazon EC2 instance is re-started

[CORRECT] By default, user data runs only during the boot cycle when you first launch an instance

[CORRECT] By default, scripts entered as user data are executed with root user privileges

Q35: A wildlife research organization uses IoT-based motion sensors attached to thousands of migrating animals to monitor their movement across regions. Every few minutes, a sensor checks for significant movement and sends updated location data to a backend application running on Amazon EC2 instances spread across multiple Availability Zones in a single AWS Region. Recently, an unexpected surge in motion data overwhelmed the application, leading to lost location records with no mechanism to replay missed data. A solutions architect must redesign the ingestion mechanism to prevent future data loss and to minimize operational overhead. What should the solutions architect do to meet these requirements?

[ ] Implement an AWS IoT Core rule to route location updates directly from each sensor to Amazon SNS. Configure the application to poll the SNS topic for new messages

[CORRECT] Create an Amazon Simple Queue Service (Amazon SQS) queue to buffer the incoming location data. Configure the backend application to poll the queue and process messages

[ ] Deploy an Amazon Data Firehose delivery stream to collect the motion data. Configure it to deliver data to an S3 bucket where the application scans and processes the files periodically

[ ] Set up a containerized service using Amazon ECS with an internal queue built into the application layer. Configure the motion sensors to send location updates directly to the container endpoints

Q36: A financial services company has developed its flagship application on AWS Cloud with data security requirements such that the encryption key must be stored in a custom application running on-premises. The company wants to offload the data storage as well as the encryption process to Amazon S3 but continue to use the existing encryption key. Which of the following Amazon S3 encryption options allows the company to leverage Amazon S3 for storing data with given constraints?

[CORRECT] Server-Side Encryption with Customer-Provided Keys (SSE-C)

[ ] Client-Side Encryption with data encryption is done on the client-side before sending it to Amazon S3

[ ] Server-Side Encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS)

[ ] Server-Side Encryption with Amazon S3 managed keys (SSE-S3)

Q37: A company has historically operated only in theus-east-1region and stores encrypted data in Amazon S3 using SSE-KMS. As part of enhancing its security posture as well as improving the backup and recovery architecture, the company wants to store the encrypted data in Amazon S3 that is replicated into theus-west-1AWS region. The security policies mandate that the data must be encrypted and decrypted using the same key in both AWS regions. Which of the following represents the best solution to address these requirements?

[ ] Enable replication for the current bucket in us-east-1 region into another bucket in us-west-1 region. Share the existing AWS KMS key from us-east-1 region to us-west-1 region

[ ] Create an Amazon CloudWatch scheduled rule to invoke an AWS Lambda function to copy the daily data from the source bucket in us-east-1 region to the destination bucket in us-west-1 region. Provide AWS KMS key access to the AWS Lambda function for encryption and decryption operations on the data in the source and destination Amazon S3 buckets

[ ] Change the AWS KMS single region key used for the current Amazon S3 bucket into an AWS KMS multi-region key. Enable Amazon S3 batch replication for the existing data in the current bucket in us-east-1 region into another bucket in us-west-1 region

[CORRECT] Create a new Amazon S3 bucket in the us-east-1 region with replication enabled from this new bucket into another bucket in us-west-1 region. Enable SSE-KMS encryption on the new bucket in us-east-1 region by using an AWS KMS multi-region key. Copy the existing data from the current Amazon S3 bucket in us-east-1 region into this new Amazon S3 bucket in us-east-1 region

Q38: A media publishing company is migrating its legacy content management application to AWS. Currently, the application and its MySQL database run on a single on-premises virtual machine, which creates a single point of failure and limits scalability. As traffic has increased due to growing reader engagement and video uploads, the company needs to redesign the solution to ensure automatic scaling, high availability, and separation of application and database layers. The company wants to continue using a MySQL-compatible engine and needs a cost-effective, managed solution that minimizes operational overhead. Which AWS architecture will best fulfill these requirements?

[ ] Host the application on EC2 instances that are part of a target group for an Application Load Balancer. Create an Amazon RDS for MySQL Multi-AZ DB instance to provide high availability and automatic failover for the database

[ ] Containerize the application and deploy it to Amazon ECS with EC2 launch type behind an Application Load Balancer. Use Amazon Neptune to store structured relational data with SQL-like queries

[ ] Deploy the application to EC2 instances registered in a Network Load Balancer target group. Use Amazon ElastiCache for Redis as the database and configure it with Redis Streams for persistent storage

[CORRECT] Migrate the application to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. Use Amazon Aurora Serverless v2 for MySQL to manage the database layer with auto-scaling and built-in high availability

Q39: Consider the following policy associated with an IAM group containing several users: Which of the following options is correct?

[ ] Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the EC2 instance's IP address is 10.200.200.200

[CORRECT] Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200

[ ] Users belonging to the IAM user group can terminate an Amazon EC2 instance belonging to any region except the us-west-1 region when the user's source IP is 10.200.200.200

[ ] Users belonging to the IAM user group cannot terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200

Q40: A Hollywood studio is planning a series of promotional events leading up to the launch of the trailer of its next sci-fi thriller. The executives at the studio want to create a static website with lots of animations in line with the theme of the movie. The studio has hired you as a solutions architect to build a scalable serverless solution. Which of the following represents the MOST cost-optimal and high-performance solution?

[CORRECT] Build the website as a static website hosted on Amazon S3. Create an Amazon CloudFront distribution with Amazon S3 as the origin. Use Amazon Route 53 to create an alias record that points to your Amazon CloudFront distribution

[ ] Host the website on AWS Lambda. Create an Amazon CloudFront distribution with Lambda as the origin

[ ] Host the website on an instance in the studio's on-premises data center. Create an Amazon CloudFront distribution with this instance as the custom origin

[ ] Host the website on an Amazon EC2 instance. Create a Amazon CloudFront distribution with the Amazon EC2 instance as the custom origin

Q41: A media company has created an AWS Direct Connect connection for migrating its flagship application to the AWS Cloud. The on-premises application writes hundreds of video files into a mounted NFS file system daily. Post-migration, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system. Before the migration cutover, the company must build a process that will replicate the newly created on-premises video files to the Amazon EFS file system. Which of the following represents the MOST operationally efficient way to meet this requirement?

[ ] Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using a VPC gateway endpoint for Amazon S3. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system

[ ] Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS VPC peering endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours

[CORRECT] Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours

[ ] Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using public VIF. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system

Q42: A video conferencing platform serves users worldwide through a globally distributed deployment of Amazon EC2 instances behind Network Load Balancers (NLBs) in several AWS Regions. The platform's architecture currently allows clients to connect to any Region via public endpoints, depending on how DNS resolves. However, users in regions far from the load balancers frequently experience high latency and slow connection times, especially during session initiation. The company wants to optimize the experience for global users by reducing end-to-end latency and load time while keeping the existing NLBs and EC2-based application infrastructure in place. Which solution will best meet these requirements?

[ ] Replace all Network Load Balancers (NLBs) with Application Load Balancers (ALBs) in each Region. Register the EC2 instances as targets behind the ALBs and use cross-zone load balancing for latency distribution

[ ] Deploy Amazon CloudFront with HTTP caching enabled in front of the NLBs. Use CloudFront edge locations to serve user requests faster and reduce the load on the backend EC2 instances

[ ] Configure Amazon Route 53 with latency-based routing policies to direct users to the Region with the lowest response time. Use health checks to fail over to another Region if a specific NLB becomes unhealthy

[CORRECT] Deploy a standard accelerator in AWS Global Accelerator and register the existing regional NLBs as endpoints. Use the accelerator to route user requests through AWS's global edge network to the closest healthy Regional NLB

Q43: An analytics company wants to improve the performance of its big data processing workflows running on Amazon Elastic File System (Amazon EFS). Which of the following performance modes should be used for Amazon EFS to address this requirement?

[ ] General Purpose

[ ] Bursting Throughput

[ ] Provisioned Throughput

[CORRECT] Max I/O

Q44: An application runs big data workloads on Amazon Elastic Compute Cloud (Amazon EC2) instances. The application runs 24x7 all round the year and needs at least 20 instances to maintain a minimum acceptable performance threshold and the application needs 300 instances to handle spikes in the workload. Based on historical workloads processed by the application, it needs 80 instances 80% of the time. As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution so that it can meet the workload demand in a steady state?

[CORRECT] Purchase 80 reserved instances (RIs). Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)

[ ] Purchase 80 spot instances. Use Auto Scaling Group to provision the remaining instances as on-demand instances per the workload demand

[ ] Purchase 20 on-demand instances. Use Auto Scaling Group to provision the remaining instances as spot instances per the workload demand

[ ] Purchase 80 on-demand instances. Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with launch template to provision the mix of on-demand and spot instances)

Q45: What does this IAM policy do?

[ ] It allows running Amazon EC2 instances in the eu-west-1 region, when the API call is made from the eu-west-1 region

[ ] It allows running Amazon EC2 instances in any region when the API call is originating from the eu-west-1 region

[ ] It allows running Amazon EC2 instances anywhere but in the eu-west-1 region

[CORRECT] It allows running Amazon EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world

Q46: A financial institution is transitioning its critical back-office systems to AWS. These systems currently rely on Microsoft SQL Server databases hosted on on-premises infrastructure. The data is highly sensitive and subject to regulatory compliance. The organization wants to enhance security and minimize database management tasks as part of the migration. Which solution will best meet these goals with the least operational burden?

[ ] Move the SQL Server data into Amazon Timestream to gain time series insights. Use AWS CloudTrail to monitor access to the data

[CORRECT] Migrate the SQL Server databases to a Multi-AZ Amazon RDS for SQL Server deployment. Enable encryption at rest by using an AWS Key Management Service (AWS KMS) managed key

[ ] Migrate the SQL Server databases to Amazon EC2 instances with encrypted EBS volumes. Use an AWS KMS customer managed key to enable encryption

[ ] Export the SQL Server databases to CSV format and store them in Amazon S3 with S3 bucket policies for access control. Use AWS Backup for data protection

Q47: A silicon valley based startup has a two-tier architecture using Amazon EC2 instances for its flagship application. The web servers (listening on port 443), which have been assigned security group A, are in public subnets across two Availability Zones (AZs) and the MSSQL based database instances (listening on port 1433), which have been assigned security group B, are in two private subnets across two Availability Zones (AZs). The DevOps team wants to review the security configurations of the application architecture. As a solutions architect, which of the following options would you select as the MOST secure configuration? (Select two)

[ ] For security group B: Add an inbound rule that allows traffic only from security group A on port 443

[ ] For security group B: Add an inbound rule that allows traffic only from all sources on port 1433

[ ] For security group A: Add an inbound rule that allows traffic from all sources on port 443. Add an outbound rule with the destination as security group B on port 443

[CORRECT] For security group A: Add an inbound rule that allows traffic from all sources on port 443. Add an outbound rule with the destination as security group B on port 1433

[CORRECT] For security group B: Add an inbound rule that allows traffic only from security group A on port 1433

Q48: An e-commerce company operates multiple AWS accounts and has interconnected these accounts in a hub-and-spoke style using the AWS Transit Gateway. Amazon Virtual Private Cloud (Amazon VPCs) have been provisioned across these AWS accounts to facilitate network isolation. Which of the following solutions would reduce both the administrative overhead and the costs while providing shared access to services required by workloads in each of the VPCs?

[CORRECT] Build a shared services Amazon Virtual Private Cloud (Amazon VPC)

[ ] Use VPCs connected with AWS Direct Connect

[ ] Use Fully meshed VPC Peering connection

[ ] Use Transit VPC to reduce cost and share the resources across Amazon Virtual Private Cloud (Amazon VPCs)

Q49: A financial services company has deployed its flagship application on Amazon EC2 instances. Since the application handles sensitive customer data, the security team at the company wants to ensure that any third-party Secure Sockets Layer certificate (SSL certificate) SSL/Transport Layer Security (TLS) certificates configured on Amazon EC2 instances via the AWS Certificate Manager (ACM) are renewed before their expiry date. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution that notifies the security team 30 days before the certificate expiration. The solution should require the least amount of scripting and maintenance effort. What will you recommend?

[ ] Monitor the days to expiry Amazon CloudWatch metric for certificates created via ACM. Create a CloudWatch alarm to monitor such certificates based on the days to expiry metric and then trigger a custom action of notifying the security team

[ ] Monitor the days to expiry Amazon CloudWatch metric for certificates imported into ACM. Create a CloudWatch alarm to monitor such certificates based on the days to expiry metric and then trigger a custom action of notifying the security team

[CORRECT] Leverage AWS Config managed rule to check if any third-party SSL/TLS certificates imported into ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

[ ] Leverage AWS Config managed rule to check if any SSL/TLS certificates created via ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

Q50: What does this IAM policy do?

[ ] It allows starting an Amazon EC2 instance only when they have a Private IP within the 34.50.31.0/24 CIDR block

[CORRECT] It allows starting an Amazon EC2 instance only when the IP where the call originates is within the 34.50.31.0/24 CIDR block

[ ] It allows starting an Amazon EC2 instance only when they have an Elastic IP within the 34.50.31.0/24 CIDR block

[ ] It allows starting an Amazon EC2 instance only when they have a Public IP within the 34.50.31.0/24 CIDR block

Q51: A financial services company runs a Kubernetes-based microservices application in its on-premises data center. The application uses the Advanced Message Queuing Protocol (AMQP) to interact with a message queue. The company is experiencing rapid growth and its on-prem infrastructure cannot scale fast enough. The company wants to migrate the application to AWS with minimal code changes and reduce infrastructure management overhead. The messaging component must continue using AMQP, and the solution should offer high scalability and low operational effort. Which combination of options will together meet these requirements? (Select two)

[CORRECT] Deploy the containerized application to Amazon Elastic Kubernetes Service (Amazon EKS) using AWS Fargate to avoid managing EC2 nodes

[CORRECT] Replace the current messaging system with Amazon MQ, a fully managed broker that supports AMQP natively. Integrate the application with the Amazon MQ endpoint without modifying the existing message format

[ ] Use Amazon Simple Queue Service (Amazon SQS) as the replacement for the AMQP message broker. Refactor the application to use SQS SDKs and polling logic

[ ] Deploy the application to Amazon ECS on EC2, and integrate the messaging workflow using Amazon SNS for asynchronous pub/sub delivery

[ ] Run the application on Amazon EC2 Auto Scaling groups and use a self-hosted RabbitMQ instance on EC2 to preserve AMQP compatibility

Q52: To improve the performance and security of the application, the engineering team at a company has created an Amazon CloudFront distribution with an Application Load Balancer as the custom origin. The team has also set up an AWS Web Application Firewall (AWS WAF) with Amazon CloudFront distribution. The security team at the company has noticed a surge in malicious attacks from a specific IP address to steal sensitive data stored on the Amazon EC2 instances. As a solutions architect, which of the following actions would you recommend to stop the attacks?

[ ] Create a deny rule for the malicious IP in the Security Groups associated with each of the instances

[CORRECT] Create an IP match condition in the AWS WAF to block the malicious IP address

[ ] Create a ticket with AWS support to take action against the malicious IP

[ ] Create a deny rule for the malicious IP in the network access control list (network ACL) associated with each of the instances

Q53: A SaaS company is modernizing one of its legacy web applications by migrating it to AWS. The company aims to improve the availability of the application during both normal and peak traffic periods. Additionally, the company wants to implement protection against common web exploits and malicious traffic. The architecture must be scalable and integrate AWS WAF to secure incoming traffic. Which solution will best meet these requirements with high availability and minimal configuration complexity?

[ ] Launch EC2 instances in a single Availability Zone and configure AWS Global Accelerator to route traffic to the instances. Attach AWS WAF to Global Accelerator for application protection

[ ] Create an Auto Scaling group with EC2 instances in multiple Availability Zones. Attach a Network Load Balancer (NLB) to distribute incoming traffic. Integrate AWS WAF directly with the Auto Scaling group for traffic filtering

[ ] Launch two EC2 instances in separate Availability Zones and register them as targets of an Application Load Balancer. Associate the ALB with AWS WAF to filter incoming traffic

[CORRECT] Deploy the application on multiple Amazon EC2 instances in an Auto Scaling group that spans two Availability Zones. Place an Application Load Balancer (ALB) in front of the group. Associate AWS WAF with the ALB

Q54: You would like to use AWS Snowball to move on-premises backups into a long term archival tier on AWS. Which solution provides the MOST cost savings?

[ ] Create an AWS Snowball job and target a Amazon S3 Glacier Vault

[CORRECT] Create an AWS Snowball job and target an Amazon S3 bucket. Create a lifecycle policy to transition this data to Amazon S3 Glacier Deep Archive on the same day

[ ] Create an AWS Snowball job and target an Amazon S3 bucket. Create a lifecycle policy to transition this data to Amazon S3 Glacier on the same day

[ ] Create a AWS Snowball job and target an Amazon S3 Glacier Deep Archive Vault

Q55: A developer needs to implement an AWS Lambda function in AWS account A that accesses an Amazon Simple Storage Service (Amazon S3) bucket in AWS account B. As a Solutions Architect, which of the following will you recommend to meet this requirement?

[ ] The Amazon S3 bucket owner should make the bucket public so that it can be accessed by the AWS Lambda function in the other AWS account

[ ] Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the AWS Lambda function cross-account access to the Amazon S3 bucket

[CORRECT] Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role

[ ] AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda

Q56: A company is developing a global healthcare application that requires the least possible latency for database read/write operations from users in several geographies across the world. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora that offers an effective recovery point objective (RPO) of seconds and a recovery time objective (RTO) of a minute. Which of the following options would you recommend?

[ ] Set up an Amazon Aurora provisioned Database cluster

[CORRECT] Set up an Amazon Aurora Global Database cluster

[ ] Set up an Amazon Aurora multi-master Database cluster

[ ] Set up an Amazon Aurora serverless Database cluster

Q57: An e-commerce application uses an Amazon Aurora Multi-AZ deployment for its database. While analyzing the performance metrics, the engineering team has found that the database reads are causing high input/output (I/O) and adding latency to the write requests against the database. As an AWS Certified Solutions Architect Associate, what would you recommend to separate the read requests from the write requests?

[ ] Activate read-through caching on the Amazon Aurora database

[CORRECT] Set up a read replica and modify the application to use the appropriate endpoint

[ ] Provision another Amazon Aurora database and link it to the primary database as a read replica

[ ] Configure the application to read from the Multi-AZ standby instance

Q58: A company is looking at storing their less frequently accessed files on AWS that can be concurrently accessed by hundreds of Amazon EC2 instances. The company needs the most cost-effective file storage service that provides immediate access to data whenever needed. Which of the following options represents the best solution for the given requirements?

[CORRECT] Amazon Elastic File System (EFS) Standard–IA storage class

[ ] Amazon Elastic Block Store (EBS)

[ ] Amazon Elastic File System (EFS) Standard storage class

[ ] Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class

Q59: A global media agency is developing a cultural analysis project to explore how major sports stories have evolved over the last five years. The team has collected thousands of archived news bulletins and magazine spreads stored in PDF format. These documents are rich in unstructured text and come from various sources with differing layouts and font styles. The agency wants to better understand how public tone and narrative have shifted over time. The team has chosen to use Amazon Textract for its ability to accurately extract printed and scanned text from complex PDF layouts. They need a solution that can then analyze the emotional tone and subject matter of the extracted text with the least possible operational burden, using fully managed AWS services where possible. Which solution will best meet these requirements?

[ ] Process the extracted output with AWS Lambda to convert the text into CSV format. Query the data using Amazon Athena and visualize it using Amazon QuickSight.

[ ] Ingest the extracted data into Amazon Redshift using AWS Glue, and use Amazon Rekognition to analyze the tone of the document layouts for sentiment classification.

[CORRECT] Send the extracted text to Amazon Comprehend for entity detection and sentiment analysis. Store the results in Amazon S3 for further access or visualization.

[ ] Use Amazon SageMaker to train a custom sentiment analysis model. Store the model outputs in Amazon DynamoDB for structured querying by analysts

Q60: A security consultant is designing a solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Since the individual developers will have AWS account root user-level access to their own accounts, the consultant wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified. Which of the following actions meets the given requirements?

[ ] Set up an IAM policy that prohibits changes to AWS CloudTrail and attach it to the root user

[ ] Set up a service-linked role for AWS CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account

[ ] Configure a new trail in AWS CloudTrail from within the developer accounts with the organization trails option enabled

[CORRECT] Set up a service control policy (SCP) that prohibits changes to AWS CloudTrail, and attach it to the developer accounts

Q61: A mobile app allows users to submit photos, which are stored in an Amazon S3 bucket. Currently, a batch of Amazon EC2 Spot Instances is launched nightly to process all the day's uploads. Each photo requires approximately 3 minutes and 512 MB of memory to process. To improve responsiveness and minimize costs, the company wants to shift to near real-time image processing that begins as soon as an image is uploaded. Which solution will provide the MOST cost-effective and scalable architecture to meet these new requirements?

[ ] Set up Amazon S3 to push events to an Amazon SQS queue. Launch a single EC2 Reserved Instance that continuously polls the queue and processes each image upon receipt

[CORRECT] Configure Amazon S3 to send event notifications to an Amazon SQS queue each time a photo is uploaded. Set up an AWS Lambda function to poll the queue and process images asynchronously

[ ] Enable S3 event notifications to invoke an Amazon EventBridge rule. Configure an AWS Step Functions workflow to initiate an Fargate task in Amazon ECS to process the image

[ ] Configure S3 to trigger an AWS App Runner service directly. Deploy a containerized image-processing application to App Runner to automatically process each upload

Q62: A big data consulting firm needs to set up a data lake on Amazon S3 for a Health-Care client. The data lake is split in raw and refined zones. For compliance reasons, the source data needs to be kept for a minimum of 5 years. The source data arrives in the raw zone and is then processed via an AWS Glue based extract, transform, and load (ETL) job into the refined zone. The business analysts run ad-hoc queries only on the data in the refined zone using Amazon Athena. The team is concerned about the cost of data storage in both the raw and refined zones as the data is increasing at a rate of 1 terabyte daily in each zone. As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution? (Select two)

[CORRECT] Setup a lifecycle policy to transition the raw zone data into Amazon S3 Glacier Deep Archive after 1 day of object creation

[ ] Use AWS Glue ETL job to write the transformed data in the refined zone using CSV format

[CORRECT] Use AWS Glue ETL job to write the transformed data in the refined zone using a compressed file format

[ ] Setup a lifecycle policy to transition the refined zone data into Amazon S3 Glacier Deep Archive after 1 day of object creation

[ ] Create an AWS Lambda function based job to delete the raw zone data after 1 day

Q63: A health-care solutions company wants to run their applications on single-tenant hardware to meet regulatory guidelines. Which of the following is the MOST cost-effective way of isolating their Amazon Elastic Compute Cloud (Amazon EC2)instances to a single tenant?

[ ] Spot Instances

[ ] On-Demand Instances

[ ] Dedicated Hosts

[CORRECT] Dedicated Instances

Q64: The DevOps team at a major financial services company uses Multi-Availability Zone (Multi-AZ) deployment for its MySQL Amazon RDS database in order to automate its database replication and augment data durability. The DevOps team has scheduled a maintenance window for a database engine level upgrade for the coming weekend. Which of the following is the correct outcome during the maintenance window?

[ ] Any database engine level upgrade for an Amazon RDS database instance with Multi-AZ deployment triggers the primary database instance to be upgraded which is then followed by the upgrade of the standby database instance. This does not cause any downtime for the duration of the upgrade

[CORRECT] Any database engine level upgrade for an Amazon RDS database instance with Multi-AZ deployment triggers both the primary and standby database instances to be upgraded at the same time. This causes downtime until the upgrade is complete

[ ] Any database engine level upgrade for an Amazon RDS database instance with Multi-AZ deployment triggers the standby database instance to be upgraded which is then followed by the upgrade of the primary database instance. This does not cause any downtime for the duration of the upgrade

[ ] Any database engine level upgrade for an Amazon RDS database instance with Multi-AZ deployment triggers both the primary and standby database instances to be upgraded at the same time. However, this does not cause any downtime until the upgrade is complete

Q65: Your company has an on-premises Distributed File System Replication (DFSR) service to keep files synchronized on multiple Windows servers, and would like to migrate to AWS cloud. What do you recommend as a replacement for the DFSR?

[ ] Amazon Simple Storage Service (Amazon S3)

[ ] Amazon Elastic File System (Amazon EFS)

[CORRECT] Amazon FSx for Windows File Server

[ ] Amazon FSx for Lustre