AWS Certified Solutions Architect – Associate

SAA-C03

Disclaimer: This content is for educational purposes. Accuracy is attempted but not guaranteed.

No job outcome is promised.

Question 1:
A company is migrating its workloads to AWS. The company has sensitive and critical data in on-premises relational databases that run on SQL Server instances. The company wants to use the AWS Cloud to increase security and reduce operational overhead for the databases. Which solution will meet these requirements?

Options:
A. Migrate the databases to Amazon EC2 instances. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
B. Migrate the databases to a Multi-AZ Amazon RDS for SQL Server DB instance. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
C. Migrate the data to an Amazon S3 bucket. Use Amazon Macie to ensure data security.
D. Migrate the databases to an Amazon DynamoDB table. Use Amazon CloudWatch Logs to ensure data security.

Answer: B

Explanation:

- A: Wrong because EC2 requires manual management of SQL Server, patching, backups, and increases overhead.

- B: Correct because RDS with Multi-AZ is managed, secure, supports KMS encryption, and reduces overhead.

- C: Wrong because S3 is object storage, not a relational database solution.

- D: Wrong because DynamoDB is NoSQL and does not support SQL Server workloads.

Question 2:
A company wants to migrate an application to AWS. The company wants to increase the application's current availability. The company wants to use AWS WAF in the application's architecture. Which solution will meet these requirements?

Options:
A. Create an Auto Scaling group that contains multiple Amazon EC2 instances that host the application across two Availability Zones. Configure an Application Load Balancer (ALB) and set the Auto Scaling group as the target. Connect a WAF to the ALB.
B. Create a cluster placement group that contains multiple Amazon EC2 instances that hosts the application. Configure an Application Load Balancer and set the EC2 instances as the targets. Connect a WAF to the placement group.
C. Create two Amazon EC2 instances that host the application across two Availability Zones. Configure the EC2 instances as the targets of an Application Load Balancer (ALB). Connect a WAF to the ALB.
D. Create an Auto Scaling group that contains multiple Amazon EC2 instances that host the application across two Availability Zones. Configure an Application Load Balancer (ALB) and set the Auto Scaling group as the target. Connect a WAF to the Auto Scaling group.

Answer: A

Explanation:

- A: Correct because ALB + Auto Scaling across AZs provides high availability, and WAF integrates at ALB level.

- B: Wrong because placement groups are for network optimization, not availability across AZs.

- C: Wrong because it lacks scaling; only static instances.

- D: Wrong because WAF attaches to ALB, not to Auto Scaling groups.

Question 3:
A company manages a data lake in an Amazon S3 bucket that numerous applications accesses. The S3 bucket contains a unique prefix for each application. The company wants to restrict each application to its specific prefix and to have granular control of the objects under each prefix. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create dedicated S3 access points and access point policies for each application.
B. Create an S3 Batch Operations job to set the ACL permissions for each object in the S3 bucket.
C. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create replication rules by prefix.
D. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create dedicated S3 access points for each application.

Answer: A

Explanation:

- A: Correct because S3 Access Points allow prefix-based access control with minimal overhead.

- B: Wrong because ACLs are legacy and add complexity.

- C: Wrong because replication increases cost and management burden.

- D: Wrong because replication is unnecessary when access points already provide control.

Question 4:
A company has an application that customers use to upload images to an Amazon S3 bucket. Each night, the company launches an Amazon EC2 Spot Fleet that processes all the images that the company received that day. The processing for each image takes 2 minutes and requires 512 MB of memory. A solutions architect needs to change the application to process the images when the images are uploaded. Which change will meet these requirements MOST cost-effectively?

Options:
A. Use S3 Event Notifications to write a message with image details to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an AWS Lambda function to read the messages from the queue and to process the images.
B. Use S3 Event Notifications to write a message with image details to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an EC2 Reserved Instance to read the messages from the queue and to process the images.
C. Use S3 Event Notifications to publish a message with image details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure a container instance in Amazon Elastic Container Service (Amazon ECS) to subscribe to the topic and to process the images.
D. Use S3 Event Notifications to publish a message with image details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Elastic Beanstalk application to subscribe to the topic and to process the images.

Answer: A

Explanation:

- A: Correct because S3 → SQS → Lambda is serverless, event-driven, cost-effective, and scales automatically.

- B: Wrong because Reserved Instances add cost and require management.

- C: Wrong because ECS is heavier and unnecessary for simple image processing.

- D: Wrong because Elastic Beanstalk adds extra complexity and cost.

Question 5:
A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on Amazon EC2 instances in different AWS Regions and a stateless UDP-based workload hosted on premises. Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

Options:
A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.
B. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the load balancers.
C. Configure two Application Load Balancers in each Region. The first will route to the EC2 endpoints, and the second will route to the on-premises endpoints.
D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.
E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints.

Answer: AD

Explanation:

- A: Correct because AWS Global Accelerator improves performance and availability for TCP workloads globally.

- B: Wrong because CloudFront is only for HTTP/HTTPS traffic, not TCP/UDP.

- C: Wrong because ALB cannot handle UDP-based workloads.

- D: Correct because NLB supports TCP and UDP, improving hybrid workload performance.

- E: Wrong because ALB does not support UDP traffic.

Question 6:
A company runs a self-managed Microsoft SQL Server on Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS). Daily snapshots are taken of the EBS volumes. Recently, all the company's EBS snapshots were accidentally deleted while running a snapshot cleaning script that deletes all expired EBS snapshots. A solutions architect needs to update the architecture to prevent data loss without retaining EBS snapshots indefinitely. Which solution will meet these requirements with the LEAST development effort?

Options:
A. Change the IAM policy of the user to deny EBS snapshot deletion.
B. Copy the EBS snapshots to another AWS Region after completing the snapshots daily.
C. Create a 7-day EBS snapshot retention rule in Recycle Bin and apply the rule for all snapshots.
D. Copy EBS snapshots to Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

Answer: C

Explanation:

- A: Wrong because blocking deletions may prevent necessary lifecycle cleanup.

- B: Wrong because copying to another Region increases cost and doesn't solve accidental deletion in primary Region.

- C: Correct because Recycle Bin protects snapshots with retention rules, preventing accidental loss.

- D: Wrong because snapshots cannot be directly copied to S3.

Question 7:
A company wants to use an AWS CloudFormation stack for its application in a test environment. The company stores the CloudFormation template in an Amazon S3 bucket that blocks public access. The company wants to grant CloudFormation access to the template in the S3 bucket based on specific user requests to create the test environment. The solution must follow security best practices. Which solution will meet these requirements?

Options:
A. Create a gateway VPC endpoint for Amazon S3. Configure the CloudFormation stack to use the S3 object URL.
B. Create an Amazon API Gateway REST API that has the S3 bucket as the target. Configure the CloudFormation stack to use the API Gateway URL.
C. Create a presigned URL for the template object. Configure the CloudFormation stack to use the presigned URL.
D. Allow public access to the template object in the S3 bucket. Block the public access after the test environment is created.

Answer: C

Explanation:

- A: Wrong because S3 VPC endpoint doesn't grant CloudFormation direct access without permissions.

- B: Wrong because API Gateway adds unnecessary complexity.

- C: Correct because presigned URLs provide temporary, secure access to private S3 objects.

- D: Wrong because enabling public access violates best practices.

Question 8:
A company has applications that run in an organization in AWS Organizations. The company outsources operational support of the applications. The company needs to provide access for the external support engineers without compromising security. The external support engineers need access to the AWS Management Console. The external support engineers also need operating system access to the company's fleet of Amazon EC2 instances that run Amazon Linux in private subnets. Which solution will meet these requirements MOST securely?

Options:
A. Confirm that AWS Systems Manager Agent (SSM Agent) is installed on all instances. Assign an instance profile with the necessary policy to connect to Systems Manager. Use AWS IAM Identity Center to provide the external support engineers console access. Use Systems Manager Session Manager to assign the required permissions.
B. Confirm that AWS Systems Manager Agent (SSM Agent) is installed on all instances. Assign an instance profile with the necessary policy to connect to Systems Manager. Use Systems Manager Session Manager to provide local IAM user credentials in each AWS account to the external support engineers for console access.
C. Confirm that all instances have a security group that allows SSH access only from the external support engineers' source IP address ranges. Provide local IAM user credentials in each AWS account to the external support engineers for console access. Provide each external support engineer an SSH key pair to log in to the application instances.
D. Create a bastion host in a public subnet. Set up the bastion host security group to allow access from only the external engineers' IP address ranges. Ensure that all instances have a security group that allows SSH access from the bastion host. Provide each external support engineer an SSH key pair to log in to the application instances. Provide local account IAM user credentials to the engineers for console access.

Answer: A

Explanation:

- A: Correct because IAM Identity Center + SSM Session Manager provides secure console and OS access without SSH.

- B: Wrong because creating local IAM users increases management overhead.

- C: Wrong because direct SSH access is less secure and harder to audit.

- D: Wrong because bastion hosts increase attack surface and require key management.

Question 9:
A company uses Amazon RDS for PostgreSQL to run its applications in the us-east-1 Region. The company also uses machine learning (ML) models to forecast annual revenue based on near real-time reports. The reports are generated by using the same RDS for PostgreSQL database. The database performance slows during business hours. The company needs to improve database performance. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Create a cross-Region read replica. Configure the reports to be generated from the read replica.
B. Activate Multi-AZ DB instance deployment for RDS for PostgreSQL. Configure the reports to be generated from the standby database.
C. Use AWS Data Migration Service (AWS DMS) to logically replicate data to a new database. Configure the reports to be generated from the new database.
D. Create a read replica in us-east-1. Configure the reports to be generated from the read replica.

Answer: D

Explanation:

- A: Wrong because cross-Region replicas add latency and cost.

- B: Wrong because standby in Multi-AZ is not available for reads.

- C: Wrong because DMS replication is more complex and costly.

- D: Correct because an in-Region read replica offloads reporting queries cost-effectively.

Question 10:
A company hosts its multi-tier, public web application in the AWS Cloud. The web application runs on Amazon EC2 instances, and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes. What should the solutions architect do to meet this requirement?

Options:
A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.
B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.
D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

Answer: B

Explanation:

- A: Wrong because Redshift + QuickSight adds delay and isn't real-time.

- B: Correct because detailed monitoring provides 1-minute metrics for near real-time performance visibility.

- C: Wrong because Lambda adds unnecessary complexity and latency.

- D: Wrong because Redshift is for analytics, not real-time metrics collection.

Question 11:
A company runs an application that stores and shares photos. Users upload the photos to an Amazon S3 bucket. Every day, users upload approximately 150 photos. The company wants to design a solution that creates a thumbnail of each new photo and stores the thumbnail in a second S3 bucket. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Configure an Amazon EventBridge scheduled rule to invoke a script every minute on a long-running Amazon EMR cluster. Configure the script to generate thumbnails for the photos that do not have thumbnails. Configure the script to upload the thumbnails to the second S3 bucket.
B. Configure an Amazon EventBridge scheduled rule to invoke a script every minute on a memory-optimized Amazon EC2 instance that is always on. Configure the script to generate thumbnails for the photos that do not have thumbnails. Configure the script to upload the thumbnails to the second S3 bucket.
C. Configure an S3 event notification to invoke an AWS Lambda function each time a user uploads a new photo to the application. Configure the Lambda function to generate a thumbnail and to upload the thumbnail to the second S3 bucket.
D. Configure S3 Storage Lens to invoke an AWS Lambda function each time a user uploads a new photo to the application. Configure the Lambda function to generate a thumbnail and to upload the thumbnail to a second S3 bucket.

Answer: C

Explanation:

- A: Wrong because EMR is costly and overkill for simple thumbnail creation.

- B: Wrong because an always-on EC2 instance adds unnecessary costs.

- C: Correct because S3 + Lambda provides serverless, event-driven, cost-efficient thumbnail creation.

- D: Wrong because S3 Storage Lens is for metrics/analytics, not event triggers

Question 12:
A company has stored millions of objects across multiple prefixes in an Amazon S3 bucket by using the Amazon S3 Glacier Deep Archive storage class. The company needs to delete all data older than 3 years except for a subset of data that must be retained. The company has identified the data that must be retained and wants to implement a serverless solution. Which solution will meet these requirements?

Options:
A. Use S3 Inventory to list all objects. Use the AWS CLI to create a script that runs on an Amazon EC2 instance that deletes objects from the inventory list.
B. Use AWS Batch to delete objects older than 3 years except for the data that must be retained.
C. Provision an AWS Glue crawler to query objects older than 3 years. Save the manifest file of old objects. Create a script to delete objects in the manifest.
D. Enable S3 Inventory. Create an AWS Lambda function to filter and delete objects. Invoke the Lambda function with S3 Batch Operations to delete objects by using the inventory reports.

Answer: D

Explanation:

- A: Wrong because running deletion scripts on EC2 requires manual management.

- B: Wrong because AWS Batch adds unnecessary compute cost and complexity.

- C: Wrong because Glue crawler is not suited for object age filtering.

- D: Correct because S3 Inventory + Batch Operations + Lambda is serverless and automates deletion efficiently.

Question 13:
A company is building an application on AWS. The application uses multiple AWS Lambda functions to retrieve sensitive data from a single Amazon S3 bucket for processing. The company must ensure that only authorized Lambda functions can access the data. The solution must comply with the principle of least privilege. Which solution will meet these requirements?

Options:
A. Grant full S3 bucket access to all Lambda functions through a shared IAM role.
B. Configure the Lambda functions to run within a VPC. Configure a bucket policy to grant access based on the Lambda functions' VPC endpoint IP addresses.
C. Create individual IAM roles for each Lambda function. Grant the IAM roles access to the S3 bucket. Assign each IAM role as the Lambda execution role for its corresponding Lambda function.
D. Configure a bucket policy granting access to the Lambda functions based on their function ARNs.

Answer: C

Explanation:

- A: Wrong because sharing a role violates least privilege.

- B: Wrong because access should be controlled with IAM, not just IP addresses.

- C: Correct because assigning individual IAM roles enforces least privilege securely.

- D: Wrong because bucket policy based only on ARNs is less granular and harder to manage.

Question 14:
A company has developed a non-production application that is composed of multiple microservices for each of the company's business units. A single development team maintains all the microservices. The current architecture uses a static web frontend and a Java-based backend that contains the application logic. The architecture also uses a MySQL database that the company hosts on an Amazon EC2 instance. The company needs to ensure that the application is secure and available globally. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use Amazon CloudFront and AWS Amplify to host the static web frontend. Refactor the microservices to use AWS Lambda functions that the microservices access by using Amazon API Gateway. Migrate the MySQL database to an Amazon EC2 Reserved Instance.
B. Use Amazon CloudFront and Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that the microservices access by using Amazon API Gateway. Migrate the MySQL database to Amazon RDS for MySQL.
C. Use Amazon CloudFront and Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that are in a target group behind a Network Load Balancer. Migrate the MySQL database to Amazon RDS for MySQL.
D. Use Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that are in a target group behind an Application Load Balancer. Migrate the MySQL database to an Amazon EC2 Reserved Instance.

Answer: B

Explanation:

- A: Wrong because EC2 Reserved Instance for DB requires management.

- B: Correct because CloudFront + S3 + Lambda + API Gateway + RDS reduces overhead and provides global availability.

- C: Wrong because Lambda behind NLB is not common architecture and adds complexity.

- D: Wrong because EC2 Reserved Instance for DB adds operational burden.

Question 15:
A video game company is deploying a new gaming application to its global users. The company requires a solution that will provide near real-time reviews and rankings of the players. A solutions architect must design a solution to provide fast access to the data. The solution must also ensure the data persists on disks in the event that the company restarts the application. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin. Store the player data in the S3 bucket.
B. Create Amazon EC2 instances in multiple AWS Regions. Store the player data on the EC2 instances. Configure Amazon Route 53 with geolocation records to direct users to the closest EC2 instance.
C. Deploy an Amazon ElastiCache for Redis cluster. Store the player data in the ElastiCache cluster.
D. Deploy an Amazon ElastiCache for Memcached cluster. Store the player data in the ElastiCache cluster.

Answer: C

Explanation:

- A: Wrong because S3 does not provide near real-time data access.

- B: Wrong because EC2 instances across Regions increase management overhead.

- C: Correct because Redis provides persistence + low latency + real-time ranking support.

- D: Wrong because Memcached lacks persistence.

Question 16:
A company is designing an application on AWS that processes sensitive data. The application stores and processes financial data for multiple customers. To meet compliance requirements, the data for each customer must be encrypted separately at rest by using a secure, centralized key management solution. The company wants to use AWS Key Management Service (AWS KMS) to implement encryption. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Generate a unique encryption key for each customer. Store the keys in an Amazon S3 bucket. Enable server-side encryption.
B. Deploy a hardware security appliance in the AWS environment that securely stores customer-provided encryption keys. Integrate the security appliance with AWS KMS to encrypt the sensitive data in the application.
C. Create a single AWS KMS key to encrypt all sensitive data across the application.
D. Create separate AWS KMS keys for each customer's data that have granular access control and logging enabled.

Answer: D

Explanation:

- A: Wrong because storing keys in S3 is insecure.

- B: Wrong because hardware security appliances add cost and complexity.

- C: Wrong because a single KMS key does not provide per-customer separation.

- D: Correct because separate KMS keys allow per-customer encryption and compliance.

Question 17:
A company needs to design a resilient web application to process customer orders. The web application must automatically handle increases in web traffic and application usage without affecting the customer experience or losing customer orders. Which solution will meet these requirements?

Options:
A. Use a NAT gateway to manage web traffic. Use Amazon EC2 Auto Scaling groups to receive, process, and store processed customer orders. Use an AWS Lambda function to capture and store unprocessed orders.
B. Use a Network Load Balancer (NLB) to manage web traffic. Use an Application Load Balancer to receive customer orders from the NLB. Use Amazon Redshift with a Multi-AZ deployment to store unprocessed and processed customer orders.
C. Use a Gateway Load Balancer (GWLB) to manage web traffic. Use Amazon Elastic Container Service (Amazon ECS) to receive and process customer orders. Use the GWLB to capture and store unprocessed orders. Use Amazon DynamoDB to store processed customer orders.
D. Use an Application Load Balancer to manage web traffic. Use Amazon EC2 Auto Scaling groups to receive and process customer orders. Use Amazon Simple Queue Service (Amazon SQS) to store unprocessed orders. Use Amazon RDS with a Multi-AZ deployment to store processed customer orders.

Answer: D

Explanation:

- A: Wrong because NAT gateway is not for managing web traffic.

- B: Wrong because Redshift is for analytics, not transactional order storage.

- C: Wrong because GWLB is for appliances, not standard web traffic distribution.

- D: Correct because ALB + Auto Scaling + SQS + RDS ensures scalability, reliability, and durability.

Question 18:
A company is using AWS DataSync to migrate millions of files from an on-premises system to AWS. The files are 10 KB in size on average. The company wants to use Amazon S3 for file storage. For the first year after the migration, the files will be accessed once or twice and must be immediately available. After 1 year, the files must be archived for at least 7 years. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use an archive tool to group the files into large objects. Use DataSync to migrate the objects. Store the objects in S3 Glacier Instant Retrieval for the first year. Use a lifecycle configuration to transition the files to S3 Glacier Deep Archive after 1 year with a retention period of 7 years.
B. Use an archive tool to group the files into large objects. Use DataSync to copy the objects to S3 Standard-Infrequent Access (S3 Standard-IA). Use a lifecycle configuration to transition the files to S3 Glacier Instant Retrieval after 1 year with a retention period of 7 years.
C. Configure the destination storage class for the files as S3 Glacier Instant Retrieval. Use a lifecycle policy to transition the files to S3 Glacier Flexible Retrieval after 1 year with a retention period of 7 years.
D. Configure a DataSync task to transfer the files to S3 Standard-Infrequent Access (S3 Standard-IA). Use a lifecycle configuration to transition the files to S3 Deep Archive after 1 year with a retention period of 7 years.

Answer: A

Explanation:

- A: Correct because grouping files reduces overhead, Glacier Instant Retrieval covers year 1, and Deep Archive meets 7-year compliance at lowest cost.

- B: Wrong because Glacier Instant Retrieval after 1 year is more expensive.

- C: Wrong because initial storage in Glacier Instant Retrieval is not immediately available.

- D: Wrong because storing small files individually in S3-IA is less efficient.

Question 19:
A company recently performed a lift and shift migration of its on-premises Oracle database workload to run on an Amazon EC2 memory optimized Linux instance. The EC2 Linux instance uses a 1 TB Provisioned IOPS SSD (io1) EBS volume with 64,000 IOPS. The database storage performance after the migration is slower than the performance of the on-premises database. Which solution will improve storage performance?

Options:
A. Add more Provisioned IOPS SSD (io1) EBS volumes. Use OS commands to create a Logical Volume Management (LVM) stripe.
B. Increase the Provisioned IOPS SSD (io1) EBS volume to more than 64,000 IOPS.
C. Increase the size of the Provisioned IOPS SSD (io1) EBS volume to 2 TB.
D. Change the EC2 Linux instance to a storage optimized instance type. Do not change the Provisioned IOPS SSD (io1) EBS volume.

Answer: A

Explanation:

- A: Correct because striping multiple EBS volumes improves throughput and IOPS.

- B: Wrong because 64,000 IOPS is already at the max per volume.

- C: Wrong because increasing size won't exceed IOPS max limits.

- D: Wrong because changing instance type alone won't fix EBS throughput issue.

Question 20:
A company is migrating from a monolithic architecture for a web application that is hosted on Amazon EC2 to a serverless microservices architecture. The company wants to use AWS services that support an event-driven, loosely coupled architecture. The company wants to use the publish/subscribe (pub/sub) pattern. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Configure an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon Simple Queue Service (Amazon SQS) queue. Configure one or more subscribers to read events from the SQS queue.
B. Configure an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon Simple Notification Service (Amazon SNS) topic. Configure one or more subscribers to receive events from the SNS topic.
C. Configure an Amazon API Gateway WebSocket API to write to a data stream in Amazon Kinesis Data Streams with enhanced fan-out. Configure one or more subscribers to receive events from the data stream.
D. Configure an Amazon API Gateway HTTP API to invoke an AWS Lambda function that publishes events to an Amazon Simple Notification Service (Amazon SNS) topic. Configure one or more subscribers to receive events from the topic.

Answer: D

Explanation:

- A: Wrong because SQS is point-to-point, not pub/sub.

- B: Wrong because REST API is heavier and costlier than HTTP API.

- C: Wrong because Kinesis is complex and costly for simple pub/sub.

- D: Correct because API Gateway HTTP API + SNS is lightweight, event-driven, and cost-effective.

Question 21:
A company recently migrated a monolithic application to an Amazon EC2 instance and Amazon RDS. The application has tightly coupled modules. The existing design of the application gives the application the ability to run on only a single EC2 instance. The company has noticed high CPU utilization on the EC2 instance during peak usage times. The high CPU utilization corresponds to degraded performance on Amazon RDS for read requests. The company wants to reduce the high CPU utilization and improve read request performance. Which solution will meet these requirements?

Options:
A. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Configure an RDS read replica for read requests.
B. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Add an RDS read replica and redirect all read/write traffic to the replica.
C. Configure an Auto Scaling group with a minimum size of 1 and maximum size of 2. Resize the RDS DB instance to an instance type that has more CPU capacity.
D. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Resize the RDS DB instance to an instance type that has more CPU capacity.

Answer: A

Explanation:

- A: Correct because read replicas offload read traffic while resizing EC2 improves compute.

- B: Wrong because read/write traffic cannot go to replicas.

- C: Wrong because scaling EC2 horizontally is not supported with monolith.

- D: Wrong because resizing DB won't address read load distribution.

Question 22:
A company needs to grant a team of developers access to the company's AWS resources. The company must maintain a high level of security for the resources. The company requires an access control solution that will prevent unauthorized access to the sensitive data. Which solution will meet these requirements?

Options:
A. Share the IAM user credentials for each development team member with the rest of the team to simplify access management and to streamline development workflows.
B. Define IAM roles that have fine-grained permissions based on the principle of least privilege. Assign an IAM role to each developer.
C. Create IAM access keys to grant programmatic access to AWS resources. Allow only developers to interact with AWS resources through API calls by using the access keys.
D. Create an AWS Cognito user pool. Grant developers access to AWS resources by using the user pool.

Answer: B

Explanation:

- A: Wrong because sharing credentials violates security best practices.

- B: Correct because IAM roles with least privilege enforce secure access per developer.

- C: Wrong because static access keys are risky and less secure.

- D: Wrong because Cognito is for application users, not developers.

Question 23:
A company hosts a monolithic web application on an Amazon EC2 instance. Application users have recently reported poor performance at specific times. Analysis of Amazon CloudWatch metrics shows that CPU utilization is 100% during the periods of poor performance. The company wants to resolve this performance issue and improve application availability. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

Options:
A. Use AWS Compute Optimizer to obtain a recommendation for an instance type to scale vertically.
B. Create an Amazon Machine Image (AMI) from the web server. Reference the AMI in a new launch template.
C. Create an Auto Scaling group and an Application Load Balancer to scale vertically.
D. Use AWS Compute Optimizer to obtain a recommendation for an instance type to scale horizontally.
E. Create an Auto Scaling group and an Application Load Balancer to scale horizontally.

Answer: BE

Explanation:

- A: Wrong because vertical scaling alone doesn't solve availability issues.

- B: Correct because creating AMI + launch template is needed for Auto Scaling.

- C: Wrong because Auto Scaling is horizontal, not vertical.

- D: Wrong because Compute Optimizer doesn't scale horizontally automatically.

- E: Correct because Auto Scaling + ALB enables horizontal scaling and better availability.

Question 24:
A company runs all its business applications in the AWS Cloud. The company uses AWS Organizations to manage multiple AWS accounts. A solutions architect needs to review all permissions that are granted to IAM users to determine which IAM users have more permissions than required. Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A. Use Network Access Analyzer to review all access permissions in the company's AWS accounts.
B. Create an AWS CloudWatch alarm that activates when an IAM user creates or modifies resources in an AWS account.
C. Use AWS Identity and Access Management (IAM) Access Analyzer to review all the company's resources and accounts.
D. Use Amazon Inspector to find vulnerabilities in existing IAM policies.

Answer: C

Explanation:

- A: Wrong because Network Access Analyzer is for VPC networking, not IAM.

- B: Wrong because alarms don't analyze permission levels.

- C: Correct because IAM Access Analyzer reviews permissions across accounts and resources.

- D: Wrong because Inspector is for security vulnerabilities, not IAM permissions.

Question 25:
A company needs to implement a new data retention policy for regulatory compliance. As part of this policy, sensitive documents that are stored in an Amazon S3 bucket must be protected from deletion or modification for a fixed period of time. Which solution will meet these requirements?

Options:
A. Activate S3 Object Lock on the required objects and enable governance mode.
B. Activate S3 Object Lock on the required objects and enable compliance mode.
C. Enable versioning on the S3 bucket. Set a lifecycle policy to delete the objects after a specified period.
D. Configure an S3 Lifecycle policy to transition objects to S3 Glacier Flexible Retrieval for the retention duration.

Answer: B

Explanation:

- A: Wrong because governance mode allows privileged users to bypass restrictions.

- B: Correct because compliance mode enforces WORM and cannot be overridden.

- C: Wrong because lifecycle policies don't prevent deletion during the retention period.

- D: Wrong because Glacier transition doesn't enforce immutability.

Question 26:
A company runs its customer-facing web application on containers. The workload uses Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The web application is resource intensive. The web application needs to be available 24 hours a day, 7 days a week for customers. The company expects the application to experience short bursts of high traffic. The workload must be highly available. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Configure an ECS capacity provider with Fargate. Conduct load testing by using a third-party tool. Rightsize the Fargate tasks in Amazon CloudWatch.
B. Configure an ECS capacity provider with Fargate for steady state and Fargate Spot for burst traffic.
C. Configure an ECS capacity provider with Fargate Spot for steady state and Fargate for burst traffic.
D. Configure an ECS capacity provider with Fargate. Use AWS Compute Optimizer to rightsize the Fargate task.

Answer: B

Explanation:

- A: Wrong because rightsizing alone doesn't address burst traffic cost-effectively.

- B: Correct because steady traffic on Fargate + burst traffic on cheaper Fargate Spot balances cost and availability.

- C: Wrong because Spot for steady state risks interruption.

- D: Wrong because rightsizing with Compute Optimizer doesn't cover scaling bursts.

Question 27:
A company is building an application in the AWS Cloud. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses Amazon Route 53 for the DNS. The company needs a managed solution with proactive engagement to detect against DDoS attacks. Which solution will meet these requirements?

Options:
A. Enable AWS Config. Configure an AWS Config managed rule that detects DDoS attacks.
B. Enable AWS WAF on the ALB. Create an AWS WAF web ACL with rules to detect and prevent DDoS attacks. Associate the web ACL with the ALB.
C. Store the ALB access logs in an Amazon S3 bucket. Configure Amazon GuardDuty to detect and take automated preventative actions for DDoS attacks.
D. Subscribe to AWS Shield Advanced. Configure hosted zones in Route 53. Add ALB resources as protected resources.

Answer: D

Explanation:

- A: Wrong because AWS Config checks compliance, not DDoS mitigation.

- B: Wrong because WAF protects against application-layer attacks, not volumetric DDoS.

- C: Wrong because GuardDuty is for anomaly detection, not direct DDoS prevention.

- D: Correct because Shield Advanced provides managed DDoS protection with proactive engagement.

Question 28:
A company hosts a video streaming web application in a VPC. The company uses a Network Load Balancer (NLB) to handle TCP traffic for real-time data processing. There have been unauthorized attempts to access the application. The company wants to improve application security with minimal architectural change to prevent unauthorized attempts to access the application. Which solution will meet these requirements?

Options:
A. Implement a series of AWS WAF rules directly on the NLB to filter out unauthorized traffic.
B. Recreate the NLB with a security group to allow only trusted IP addresses.
C. Deploy a second NLB in parallel with the existing NLB configured with a strict IP address allow list.
D. Use AWS Shield Advanced to provide enhanced DDoS protection and prevent unauthorized access attempts.

Answer: B

Explanation:

- A: Wrong because WAF cannot be applied directly on NLB.

- B: Correct because NLB with a security group controlling IPs is minimal change and secures access.

- C: Wrong because maintaining two NLBs is inefficient and costly.

- D: Wrong because Shield Advanced mitigates DDoS but not direct unauthorized IP access.

Question 29:
A healthcare company is developing an AWS Lambda function that publishes notifications to an encrypted Amazon Simple Notification Service (Amazon SNS) topic. The notifications contain protected health information (PHI). The SNS topic uses AWS Key Management Service (AWS KMS) customer managed keys for encryption. The company must ensure that the application has the necessary permissions to publish messages securely to the SNS topic. Which combination of steps will meet these requirements? (Choose three.)

Options:
A. Create a resource policy for the SNS topic that allows the Lambda function to publish messages to the topic.
B. Use server-side encryption with AWS KMS keys (SSE-KMS) for the SNS topic instead of customer managed keys.
C. Create a resource policy for the encryption key that the SNS topic uses that has the necessary AWS KMS permissions.
D. Specify the Lambda function's Amazon Resource Name (ARN) in the SNS topic's resource policy.
E. Associate an Amazon API Gateway HTTP API with the SNS topic to control access to the topic by using API Gateway resource policies.
F. Configure a Lambda execution role that has the necessary IAM permissions to use a customer managed key in AWS KMS.

Answer: ACF

Explanation:

- A: Correct because the SNS topic must allow the Lambda to publish.

- B: Wrong because replacing customer managed keys breaks compliance.

- C: Correct because KMS key policy must allow encryption actions.

- D: Wrong because Lambda execution role already covers identity.

- E: Wrong because API Gateway is unnecessary for direct publish.

- F: Correct because Lambda role needs IAM permissions to use the KMS CMK.

Question 30:
A company has an employee web portal. Employees log in to the portal to view payroll details. The company is developing a new system to give employees the ability to upload scanned documents for reimbursement. The company runs a program to extract text-based data from the documents and attach the extracted information to each employee's reimbursement IDs for processing. The employee web portal requires 100% uptime. The document extract program runs infrequently throughout the day on an on-demand basis. The company wants to build a scalable and cost-effective new system that will require minimal changes to the existing web portal. The company does not want to make any code changes. Which solution will meet these requirements with the LEAST implementation effort?

Options:
A. Run Amazon EC2 On-Demand Instances in an Auto Scaling group for the web portal. Use an AWS Lambda function to run the document extract program. Invoke the Lambda function when an employee uploads a new reimbursement document.
B. Run Amazon EC2 Spot Instances in an Auto Scaling group for the web portal. Run the document extract program on EC2 Spot Instances. Start document extract program instances when an employee uploads a new reimbursement document.

C. Purchase a Savings Plan to run the web portal and the document extract program. Run the web portal and the document extract program in an Auto Scaling group.
D. Create an Amazon S3 bucket to host the web portal. Use Amazon API Gateway and an AWS Lambda function for the existing functionalities. Use the Lambda function to run the document extract program. Invoke the Lambda function when the API that is associated with a new document upload is called.

Answer: D

Explanation:

- A: Wrong because migrating portal to EC2 requires changes.

- B: Wrong because Spot is unreliable for infrequent workloads needing guaranteed execution.

- C: Wrong because combining portal + extract in EC2 group is not cost-optimized.

- D: Correct because S3 hosting + API Gateway + Lambda adds scalability with minimal code changes.

Question 31:
A media company has a multi-account AWS environment in the us-east-1 Region. The company has an Amazon Simple Notification Service (Amazon SNS) topic in a production account that publishes performance metrics. The company has an AWS Lambda function in an administrator account to process and analyze log data. The Lambda function that is in the administrator account must be invoked by messages from the SNS topic that is in the production account when significant metrics are reported. Which combination of steps will meet these requirements? (Choose two.)

Options:
A. Create an IAM resource policy for the Lambda function that allows Amazon SNS to invoke the function.
B. Implement an Amazon Simple Queue Service (Amazon SQS) queue in the administrator account to buffer messages from the SNS topic that is in the production account. Configure the SQS queue to invoke the Lambda function.
C. Create an IAM policy for the SNS topic that allows the Lambda function to subscribe to the topic.
D. Use an Amazon EventBridge rule in the production account to capture the SNS topic notifications. Configure the EventBridge rule to forward notifications to the Lambda function that is in the administrator account.
E. Store performance metrics in an Amazon S3 bucket in the production account. Use Amazon Athena to analyze the metrics from the administrator account.

Answer: AB

Explanation:

- A: Correct because SNS must have permission to invoke the Lambda function.

- B: Correct because SQS decouples cross-account messaging and triggers Lambda.

- C: Wrong because IAM policy on SNS alone doesn't establish subscription.

- D: Wrong because EventBridge adds unnecessary complexity.

- E: Wrong because Athena analysis doesn't provide real-time invocation.

Question 32:
A company is migrating an application from an on-premises location to Amazon Elastic Kubernetes Service (Amazon EKS). The company must use a custom subnet for pods that are in the company's VPC to comply with requirements. The company also needs to ensure that the pods can communicate securely within the pods' VPC. Which solution will meet these requirements?

Options:
A. Configure AWS Transit Gateway to directly manage custom subnet configurations for the pods in Amazon EKS.
B. Create an AWS Direct Connect connection from the company's on-premises IP address ranges to the EKS pods.
C. Use the Amazon VPC CNI plugin for Kubernetes. Define custom subnets in the VPC cluster for the pods to use.
D. Implement a Kubernetes network policy that has pod anti-affinity rules to restrict pod placement to specific nodes that are within custom subnets.

Answer: C

Explanation:

- A: Wrong because Transit Gateway connects VPCs, not pod networking.

- B: Wrong because Direct Connect is for on-premises connectivity, not pod subnet assignment.

- C: Correct because the VPC CNI plugin allows pods to get IPs from custom VPC subnets securely.

- D: Wrong because network policies control traffic, not subnet assignment.

Question 33:
A company hosts an ecommerce application that stores all data in a single Amazon RDS for MySQL DB instance that is fully managed by AWS. The company needs to mitigate the risk of a single point of failure. Which solution will meet these requirements with the LEAST implementation effort?

Options:
A. Modify the RDS DB instance to use a Multi-AZ deployment. Apply the changes during the next maintenance window.
B. Migrate the current database to a new Amazon DynamoDB Multi-AZ deployment. Use AWS Database Migration Service (AWS DMS) with a heterogeneous migration strategy to migrate the current RDS DB instance to DynamoDB tables.
C. Create a new RDS DB instance in a Multi-AZ deployment. Manually restore the data from the existing RDS DB instance from the most recent snapshot.
D. Configure the DB instance in an Amazon EC2 Auto Scaling group with a minimum group size of three. Use Amazon Route 53 simple routing to distribute requests to all DB instances.

Answer: A

Explanation:

- A: Correct because enabling Multi-AZ on RDS is simple and adds high availability with minimal effort.

- B: Wrong because migrating to DynamoDB changes architecture significantly.

- C: Wrong because manual restore adds unnecessary work compared to enabling Multi-AZ.

- D: Wrong because databases cannot scale in Auto Scaling groups.

Question 34:
A company has multiple Microsoft Windows SMB file servers and Linux NFS file servers for file sharing in an on-premises environment. As part of the company's AWS migration plan, the company wants to consolidate the file servers in the AWS Cloud. The company needs a managed AWS storage service that supports both NFS and SMB access. The solution must be able to share between protocols. The solution must have redundancy at the Availability Zone level. Which solution will meet these requirements?

Options:
A. Use Amazon FSx for NetApp ONTAP for storage. Configure multi-protocol access.
B. Create two Amazon EC2 instances. Use one EC2 instance for Windows SMB file server access and one EC2 instance for Linux NFS file server access.
C. Use Amazon FSx for NetApp ONTAP for SMB access. Use Amazon FSx for Lustre for NFS access.
D. Use Amazon S3 storage. Access Amazon S3 through an Amazon S3 File Gateway.

Answer: A

Explanation:

- A: Correct because FSx for NetApp ONTAP supports both SMB and NFS with multi-protocol access.

- B: Wrong because EC2 file servers require self-management.

- C: Wrong because using two FSx services does not provide cross-protocol access.

- D: Wrong because S3 File Gateway is not multi-protocol with shared SMB/NFS support.

Question 35:
A software company needs to upgrade a critical web application. The application currently runs on a single Amazon EC2 instance that the company hosts in a public subnet. The EC2 instance runs a MySQL database. The application's DNS records are published in an Amazon Route 53 zone. A solutions architect must reconfigure the application to be scalable and highly available. The solutions architect must also reduce MySQL read latency. Which combination of solutions will meet these requirements? (Choose two.)

Options:
A. Launch a second EC2 instance in a second AWS Region. Use a Route 53 failover routing policy to redirect the traffic to the second EC2 instance.
B. Create and configure an Auto Scaling group to launch private EC2 instances in multiple Availability Zones. Add the instances to a target group behind a new Application Load Balancer.
C. Migrate the database to an Amazon Aurora MySQL cluster. Create the primary DB instance and reader DB instance in separate Availability Zones.
D. Create and configure an Auto Scaling group to launch private EC2 instances in multiple AWS Regions. Add the instances to a target group behind a new Application Load Balancer.
E. Migrate the database to an Amazon Aurora MySQL cluster with cross-Region read replicas.

Answer: BC

Explanation:

- A: Wrong because cross-Region failover increases latency and cost unnecessarily.

- B: Correct because Auto Scaling across AZs ensures scalability and high availability.

- C: Correct because Aurora MySQL cluster with reader instances reduces read latency.

- D: Wrong because multi-Region ALB is not supported.

- E: Wrong because cross-Region replicas are unnecessary for latency reduction.

Question 36:
A company runs thousands of AWS Lambda functions. The company needs a solution to securely store sensitive information that all the Lambda functions use. The solution must also manage the automatic rotation of the sensitive information. Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

Options:
A. Create HTTP security headers by using Lambda@Edge to retrieve and create sensitive information.
B. Create a Lambda layer that retrieves sensitive information.
C. Store sensitive information in AWS Secrets Manager.
D. Store sensitive information in AWS Systems Manager Parameter Store.
E. Create a Lambda consumer with dedicated throughput to retrieve sensitive information and create environmental variables.

Answer: CD

Explanation:

- A: Wrong because Lambda@Edge is for CDN customization, not secrets management.

- B: Wrong because Lambda layers are for code, not secrets.

- C: Correct because Secrets Manager stores sensitive data and supports automatic rotation.

- D: Correct because Parameter Store can securely store sensitive information.

- E: Wrong because creating a Lambda consumer adds overhead and is unnecessary.

Question 37:
A company has an internal application that runs on Amazon EC2 instances in an Auto Scaling group. The EC2 instances are compute optimized and use Amazon Elastic Block Store (Amazon EBS) volumes. The company wants to identify cost optimizations across the EC2 instances, the Auto Scaling group, and the EBS volumes. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A. Create a new AWS Cost and Usage Report. Search the report for cost recommendations for the EC2 instances, the Auto Scaling group, and the EBS volumes.
B. Create new Amazon CloudWatch billing alerts. Check the alert statuses for cost recommendations for the EC2 instances, the Auto Scaling group, and the EBS volumes.
C. Configure AWS Compute Optimizer for cost recommendations for the EC2 instances, the Auto Scaling group and the EBS volumes.
D. Configure AWS Compute Optimizer for cost recommendations for the EC2 instances. Create a new AWS Cost and Usage Report. Search the report for cost recommendations for the Auto Scaling group and the EBS volumes.

Answer: C

Explanation:

- A: Wrong because Cost and Usage Report gives raw billing data, not recommendations.

- B: Wrong because CloudWatch billing alerts only notify cost increases.

- C: Correct because Compute Optimizer provides automated cost recommendations for EC2, ASG, and EBS.

- D: Wrong because mixing services increases complexity and isn't efficient.

Question 38:
A company is running a media store across multiple Amazon EC2 instances distributed across multiple Availability Zones in a single VPC. The company wants a high-performing solution to share data between all the EC2 instances, and prefers to keep the data within the VPC only. What should a solutions architect recommend?

Options:
A. Create an Amazon S3 bucket and call the service APIs from each instance's application.
B. Create an Amazon S3 bucket and configure all instances to access it as a mounted volume.
C. Configure an Amazon Elastic Block Store (Amazon EBS) volume and mount it across all instances.
D. Configure an Amazon Elastic File System (Amazon EFS) file system and mount it across all instances.

Answer: D

Explanation:

- A: Wrong because S3 API calls add latency and are not a shared file system.

- B: Wrong because S3 cannot be mounted directly across instances.

- C: Wrong because EBS volumes cannot be shared across instances/AZs.

- D: Correct because EFS is scalable, high-performing, and shared across AZs within VPC.

Question 39:
A company uses an Amazon RDS for MySQL instance. To prepare for end-of-year processing, the company added a read replica to accommodate extra read-only queries from the company's reporting tool. The read replica CPU usage was 60% and the primary instance CPU usage was 60%. After end-of-year activities are complete, the read replica has a constant 25% CPU usage. The primary instance still has a constant 60% CPU usage. The company wants to rightsize the database and still provide enough performance for future growth. Which solution will meet these requirements?

Options:
A. Delete the read replica. Do not make changes to the primary instance.
B. Resize the read replica to a smaller instance size. Do not make changes to the primary instance.
C. Resize the read replica to a larger instance size. Resize the primary instance to a smaller instance size.
D. Delete the read replica. Resize the primary instance to a larger instance.

Answer: B

Explanation:

- A: Wrong because replica is still needed for reporting.

- B: Correct because resizing the replica down saves cost while maintaining availability.

- C: Wrong because replica is underutilized and doesn't need upsizing.

- D: Wrong because primary is already at high CPU usage and shouldn't be downsized.

Question 40:
A company is migrating its databases to Amazon RDS for PostgreSQL. The company is migrating its applications to Amazon EC2 instances. The company wants to optimize costs for long-running workloads. Which solution will meet this requirement MOST cost-effectively?

Options:
A. Use On-Demand Instances for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year Compute Savings Plan with the No Upfront option for the EC2 instances.
B. Purchase Reserved Instances for a 1 year term with the No Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year EC2 Instance Savings Plan with the No Upfront option for the EC2 instances.
C. Purchase Reserved Instances for a 1 year term with the Partial Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year EC2 Instance Savings Plan with the Partial Upfront option for the EC2 instances.
D. Purchase Reserved Instances for a 3 year term with the All Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 3 year EC2 Instance Savings Plan with the All Upfront option for the EC2 instances.

Answer: D

Explanation:

- A: Wrong because On-Demand is most expensive for long-running workloads.

- B: Wrong because 1 year No Upfront gives limited savings.

- C: Wrong because Partial Upfront saves less than All Upfront 3 years.

- D: Correct because 3-year All Upfront Reserved + Savings Plan gives maximum discount.

Question 41:
A company is using an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The company must ensure that Kubernetes service accounts in the EKS cluster have secure and granular access to specific AWS resources by using IAM roles for service accounts (IRSA). Which combination of solutions will meet these requirements? (Choose two.)

Options:
A. Create an IAM policy that defines the required permissions. Attach the policy directly to the IAM role of the EKS nodes.
B. Implement network policies within the EKS cluster to prevent Kubernetes service accounts from accessing specific AWS services.
C. Modify the EKS cluster's IAM role to include permissions for each Kubernetes service account. Ensure a one-to-one mapping between IAM roles and Kubernetes roles.
D. Define an IAM role that includes the necessary permissions. Annotate the Kubernetes service accounts with the Amazon Resource Name (ARN) of the IAM role.
E. Set up a trust relationship between the IAM roles for the service accounts and an OpenID Connect (OIDC) identity provider.

Answer: DE

Explanation:

- A: Wrong because attaching to node IAM role grants excessive permissions.

- B: Wrong because network policies manage pod communication, not AWS access.

- C: Wrong because modifying cluster IAM role is insecure and not granular.

- D: Correct because assigning IAM roles per service account enforces least privilege.

- E: Correct because IRSA requires OIDC trust setup for IAM role assumption.

Question 42:
A company regularly uploads confidential data to Amazon S3 buckets for analysis. The company's security policies mandate that the objects must be encrypted at rest. The company must automatically rotate the encryption key every year. The company must be able to track key rotation by using AWS CloudTrail. The company also must minimize costs for the encryption key. Which solution will meet these requirements?

Options:
A. Use server-side encryption with customer-provided keys (SSE-C).
B. Use server-side encryption with Amazon S3 managed keys (SSE-S3).
C. Use server-side encryption with AWS KMS keys (SSE-KMS).
D. Use server-side encryption with customer managed AWS KMS keys.

Answer: D

Explanation:

- A: Wrong because customer-provided keys require manual management.

- B: Wrong because SSE-S3 does not support key rotation.

- C: Wrong because AWS-managed KMS keys rotate automatically but don't provide audit visibility.

- D: Correct because customer managed KMS keys support rotation + audit logging + compliance.

Question 43:
A company has migrated several applications to AWS in the past 3 months. The company wants to know the breakdown of costs for each of these applications. The company wants to receive a regular report that includes this information. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use AWS Budgets to download data for the past 3 months into a .csv file. Look up the desired information.
B. Load AWS Cost and Usage Reports into an Amazon RDS DB instance. Run SQL queries to get the desired information.
C. Tag all the AWS resources with a key for cost and a value of the application's name. Activate cost allocation tags. Use Cost Explorer to get the desired information.
D. Tag all the AWS resources with a key for cost and a value of the application's name. Use the AWS Billing and Cost Management console to download bills for the past 3 months. Look up the desired information.

Answer: C

Explanation:

- A: Wrong because Budgets don't provide breakdown by application.

- B: Wrong because RDS adds cost and overhead.

- C: Correct because cost allocation tags + Cost Explorer provide breakdown by app cost-effectively.

- D: Wrong because bills are not granular for application-level costs.

Question 44:
An ecommerce company is preparing to deploy a web application on AWS to ensure continuous service for customers. The architecture includes a web application that the company hosts on Amazon EC2 instances, a relational database in Amazon RDS, and static assets that the company stores in Amazon S3. The company wants to design a robust and resilient architecture for the application. Which solution will meet these requirements?

Options:
A. Deploy Amazon EC2 instances in a single Availability Zone. Deploy an RDS DB instance in the same Availability Zone. Use Amazon S3 with versioning enabled to store static assets.
B. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy a Multi-AZ RDS DB instance. Use Amazon CloudFront to distribute static assets.
C. Deploy Amazon EC2 instances in a single Availability Zone. Deploy an RDS DB instance in a second Availability Zone for cross-AZ redundancy. Serve static assets directly from the EC2 instances.
D. Use AWS Lambda functions to serve the web application. Use Amazon Aurora Serverless v2 for the database. Store static assets in Amazon Elastic File System (Amazon EFS) One Zone-Infrequent Access (One Zone-IA).

Answer: B

Explanation:

- A: Wrong because single-AZ deployment is not resilient.

- B: Correct because Auto Scaling + Multi-AZ RDS + CloudFront ensures resiliency and global performance.

- C: Wrong because EC2 in a single AZ still risks downtime.

- D: Wrong because EFS One Zone-IA is not durable for production workloads.

Question 45:
An ecommerce company runs several internal applications in multiple AWS accounts. The company uses AWS Organizations to manage its AWS accounts. A security appliance in the company's networking account must inspect interactions between applications across AWS accounts. Which solution will meet these requirements?

Options:
A. Deploy a Network Load Balancer (NLB) in the networking account to send traffic to the security appliance. Configure the application accounts to send traffic to the NLB by using an interface VPC endpoint in the application accounts.
B. Deploy an Application Load Balancer (ALB) in the application accounts to send traffic directly to the security appliance.
C. Deploy a Gateway Load Balancer (GWLB) in the networking account to send traffic to the security appliance. Configure the application accounts to send traffic to the GWLB by using an interface GWLB endpoint in the application accounts.
D. Deploy an interface VPC endpoint in the application accounts to send traffic directly to the security appliance.

Answer: C

Explanation:

- A: Wrong because NLB doesn't natively integrate with security appliances across accounts.

- B: Wrong because ALB doesn't provide transparent network-level inspection.

- C: Correct because GWLB integrates security appliances and allows cross-account inspection with GWLB endpoints.

- D: Wrong because interface endpoints are for services, not appliances.

Question 46:
A company runs its production workload on an Amazon Aurora MySQL DB cluster that includes six Aurora Replicas. The company wants near-real-time reporting queries from one of its departments to be automatically distributed across three of the Aurora Replicas. Those three replicas have a different compute and memory specification from the rest of the DB cluster. Which solution meets these requirements?

Options:
A. Create and use a custom endpoint for the workload.
B. Create a three-node cluster clone and use the reader endpoint.
C. Use any of the instance endpoints for the selected three nodes.
D. Use the reader endpoint to automatically distribute the read-only workload.

Answer: A

Explanation:

- A: Correct because custom endpoints allow directing queries to specific replicas.

- B: Wrong because cloning creates a new cluster, unnecessary for this use case.

- C: Wrong because individual endpoints don't provide load balancing.

- D: Wrong because reader endpoint distributes across all replicas, not selective ones.

Question 47:
A company runs a Node.js function on a server in its on-premises data center. The data center stores data in a PostgreSQL database. The company stores the credentials in a connection string in an environment variable on the server. The company wants to migrate its application to AWS and to replace the Node.js application server with AWS Lambda. The company also wants to migrate to Amazon RDS for PostgreSQL and to ensure that the database credentials are securely managed. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Store the database credentials as a parameter in AWS Systems Manager Parameter Store. Configure Parameter Store to automatically rotate the secrets every 30 days. Update the Lambda function to retrieve the credentials from the parameter.
B. Store the database credentials as a secret in AWS Secrets Manager. Configure Secrets Manager to automatically rotate the credentials every 30 days. Update the Lambda function to retrieve the credentials from the secret.
C. Store the database credentials as an encrypted Lambda environment variable. Write a custom Lambda function to rotate the credentials. Schedule the Lambda function to run every 30 days.
D. Store the database credentials as a key in AWS Key Management Service (AWS KMS). Configure automatic rotation for the key. Update the Lambda function to retrieve the credentials from the KMS key.

Answer: B

Explanation:

- A: Wrong because Parameter Store requires additional configuration for rotation.

- B: Correct because Secrets Manager natively supports secure storage + rotation with minimal effort.

- C: Wrong because custom rotation adds operational overhead.

- D: Wrong because KMS keys rotate encryption keys, not database credentials.

Question 48:
A company wants to replicate existing and ongoing data changes from an on-premises Oracle database to Amazon RDS for Oracle. The amount of data to replicate varies throughout each day. The company wants to use AWS Database Migration Service (AWS DMS) for data replication. The solution must allocate only the capacity that the replication instance requires. Which solution will meet these requirements?

Options:
A. Configure the AWS DMS replication instance with a Multi-AZ deployment to provision instances across multiple Availability Zones.
B. Create an AWS DMS Serverless replication task to analyze and replicate the data while provisioning the required capacity.
C. Use Amazon EC2 Auto Scaling to scale the size of the AWS DMS replication instance up or down based on the amount of data to replicate.
D. Provision AWS DMS replication capacity by using Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type to analyze and replicate the data while provisioning the required capacity.

Answer: B

Explanation:

- A: Wrong because Multi-AZ improves HA, not cost optimization.

- B: Correct because DMS Serverless scales capacity automatically with workload.

- C: Wrong because EC2 Auto Scaling doesn't apply to DMS instances.

- D: Wrong because ECS/Fargate isn't needed; DMS Serverless is purpose-built.

Question 49:
A company has a multi-tier web application. The application's internal service components are deployed on Amazon EC2 instances. The internal service components need to access third-party software as a service (SaaS) APIs that are hosted on AWS. The company needs to provide secure and private connectivity from the application's internal services to the third-party SaaS application. The company needs to ensure that there is minimal public internet exposure. Which solution will meet these requirements?

Options:
A. Implement an AWS Site-to-Site VPN to establish a secure connection with the third-party SaaS provider.
B. Deploy AWS Transit Gateway to manage and route traffic between the application's VPC and the third-party SaaS provider.
C. Configure AWS PrivateLink to allow only outbound traffic from the VPC without enabling the third-party SaaS provider to establish.
D. Use AWS PrivateLink to create a private connection between the application's VPC and the third-party SaaS provider.

Answer: D

Explanation:

- A: Wrong because Site-to-Site VPN is for on-premises, not SaaS hosted on AWS.

- B: Wrong because Transit Gateway is for VPC interconnect, not SaaS connectivity.

- C: Wrong because PrivateLink works both ways, not only outbound traffic.

- D: Correct because PrivateLink provides secure, private SaaS connectivity without internet exposure.

Question 50:
A solutions architect needs to connect a company's corporate network to its VPC to allow on-premises access to its AWS resources. The solution must provide encryption of all traffic between the corporate network and the VPC at the network layer and the session layer. The solution also must provide security controls to prevent unrestricted access between AWS and the on-premises systems. Which solution meets these requirements?

Options:
A. Configure AWS Direct Connect to connect to the VPC. Configure the VPC route tables to allow and deny traffic between AWS and on premises as required.
B. Create an IAM policy to allow access to the AWS Management Console only from a defined set of corporate IP addresses. Restrict user access based on job responsibility by using an IAM policy and roles.
C. Configure AWS Site-to-Site VPN to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.
D. Configure AWS Transit Gateway to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.

Answer: C

Explanation:

- A: Wrong because Direct Connect alone does not provide encryption.

- B: Wrong because IAM policies restrict console access, not network traffic.

- C: Correct because Site-to-Site VPN provides encryption + security controls via SGs and NACLs.

- D: Wrong because Transit Gateway connects multiple networks but doesn't encrypt traffic.

Question 51:
A company has a custom application with embedded credentials that retrieves information from a database in an Amazon RDS for MySQL DB cluster. The company needs to make the application more secure with minimal programming effort. The company has created credentials on the RDS for MySQL database for the application user. Which solution will meet these requirements?

Options:
A. Store the credentials in AWS Key Management Service (AWS KMS). Create keys in AWS KMS. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
B. Store the credentials in encrypted local storage. Configure the application to load the database credentials from the local storage. Set up a credentials rotation schedule by creating a cron job.
C. Store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule by creating an AWS Lambda function for Secrets Manager.
D. Store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule in the RDS for MySQL database by using Parameter Store.

Answer: C

Explanation:

- A: Wrong because KMS manages encryption keys, not database credentials.

- B: Wrong because local storage + cron adds operational risk.

- C: Correct because Secrets Manager securely stores DB creds + rotation support with minimal code.

- D: Wrong because Parameter Store doesn't directly manage DB rotation.

Question 52:
A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing data and new data by using SQL. The company stores the data in an Amazon S3 bucket. The data must be encrypted at rest and replicated to a different AWS Region. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create a new S3 bucket that uses server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Configure Cross-Region Replication (CRR). Load the data into the new S3 bucket. Use Amazon Athena to query the data.
B. Create a new S3 bucket that uses server-side encryption with Amazon S3 managed keys (SSE-S3). Configure Cross-Region Replication (CRR). Load the data into the new S3 bucket. Use Amazon RDS to query the data.
C. Configure Cross-Region Replication (CRR) on the existing S3 bucket. Use server-side encryption with Amazon S3 managed keys (SSE-S3). Use Amazon Athena to query the data.
D. Configure S3 Cross-Region Replication (CRR) on the existing S3 bucket. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.

Answer: A

Explanation:

- A: Correct because Athena queries S3 directly, SSE-KMS (multi-Region keys) + CRR ensures encryption + replication.

- B: Wrong because RDS is not serverless SQL over S3.

- C: Wrong because SSE-S3 does not support customer-controlled key rotation.

- D: Wrong because RDS is unnecessary and higher operational overhead.

Question 53:
A company has a web application that has thousands of users. The application uses 8-10 user-uploaded images to generate AI images. Users can download the generated AI images once every 6 hours. The company also has a premium user option that gives users the ability to download the generated AI images anytime. The company uses the user-uploaded images to run AI model training twice a year. The company needs a storage solution to store the images. Which storage solution meets these requirements MOST cost-effectively?

Options:
A. Move uploaded images to Amazon S3 Glacier Deep Archive. Move premium user-generated AI images to S3 Standard. Move non-premium user-generated AI images to S3 Standard-Infrequent Access (S3 Standard-IA).
B. Move uploaded images to Amazon S3 Glacier Deep Archive. Move all generated AI images to S3 Glacier Flexible Retrieval.
C. Move uploaded images to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Move premium user-generated AI images to S3 Standard. Move non-premium user-generated AI images to S3 Standard-Infrequent Access (S3 Standard-IA).
D. Move uploaded images to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Move all generated AI images to S3 Glacier Flexible Retrieval.

Answer: A

Explanation:

- A: Correct because Glacier Deep Archive for rarely used uploads + S3 Standard/S3-IA tiering is cost-effective.

- B: Wrong because Glacier retrieval is too slow for premium users.

- C: Wrong because One Zone-IA reduces durability for important uploads.

- D: Wrong because Glacier for generated images impacts usability.

Question 54:
A company is developing machine learning (ML) models on AWS. The company is developing the ML models as independent microservices. The microservices fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the ML models through an asynchronous API. Users can send a request or a batch of requests. The company provides the ML models to hundreds of users. The usage patterns for the models are irregular. Some models are not used for days or weeks. Other models receive batches of thousands of requests at a time. Which solution will meet these requirements?

Options:
A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the ML models as AWS Lambda functions that the NLB will invoke. Use auto scaling to scale the Lambda functions based on the traffic that the NLB receives.
B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the ML models as Amazon Elastic Container Service (Amazon ECS) services that the ALB will invoke. Use auto scaling to scale the ECS cluster instances based on the traffic that the ALB receives.
C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the ML models as AWS Lambda functions that SQS events will invoke. Use auto scaling to increase the number of vCPUs for the Lambda functions based on the size of the SQS queue.

D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the ML models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Use auto scaling for Amazon ECS to scale both the cluster capacity and number of the services based on the size of the SQS queue.

Answer: D

Explanation:

- A: Wrong because Lambda cannot efficiently handle 1 GB load at cold start.

- B: Wrong because ALB + ECS services doesn't decouple workload spikes well.

- C: Wrong because Lambda is limited for large model initialization.

- D: Correct because ECS + SQS queue handles irregular workloads with batch scaling.

Question 55:
A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The application stores data in an Amazon Aurora MySQL DB cluster. The company needs to create a disaster recovery (DR) solution. The acceptable recovery time for the DR solution is up to 30 minutes. The DR solution does not need to support customer usage when the primary infrastructure is healthy. Which solution will meet these requirements?

Options:
A. Deploy the DR infrastructure in a second AWS Region with an ALB and an Auto Scaling group. Set the desired capacity and maximum capacity of the Auto Scaling group to a minimum value. Convert the Aurora MySQL DB cluster to an Aurora global database. Configure Amazon Route 53 for an active-passive failover with ALB endpoints.
B. Deploy the DR infrastructure in a second AWS Region with an ALB. Update the Auto Scaling group to include EC2 instances from the second Region. Use Amazon Route 53 to configure active-active failover. Convert the Aurora MySQL DB cluster to an Aurora global database.
C. Back up the Aurora MySQL DB cluster data by using AWS Backup. Deploy the DR infrastructure in a second AWS Region with an ALB. Update the Auto Scaling group to include EC2 instances from the second Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora MySQL DB cluster in the second Region. Restore the data from the backup.
D. Back up the infrastructure configuration by using AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Set the Auto Scaling group desired capacity to zero. Use Amazon Route 53 to configure active-passive failover. Convert the Aurora MySQL DB cluster to an Aurora global database.

Answer: A

Explanation:

- A: Correct because Aurora global DB + passive infra meets 30-min RTO cost-effectively.

- B: Wrong because active-active is unnecessary and costly.

- C: Wrong because restoring from backup would exceed RTO.

- D: Wrong because building infra from backup delays recovery.

Question 56:
A company is migrating its data processing application to the AWS Cloud. The application processes several short-lived batch jobs that cannot be disrupted. Data is generated after each batch job is completed. The data is accessed for 30 days and retained for 2 years. The company wants to keep the cost of running the application in the AWS Cloud as low as possible. Which solution will meet these requirements?

Options:
A. Migrate the data processing application to Amazon EC2 Spot Instances. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Instant Retrieval after 30 days. Set an expiration to delete the data after 2 years.
B. Migrate the data processing application to Amazon EC2 On-Demand Instances. Store the data in Amazon S3 Glacier Instant Retrieval. Move the data to S3 Glacier Deep Archive after 30 days. Set an expiration to delete the data after 2 years.
C. Deploy Amazon EC2 Spot Instances to run the batch jobs. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Flexible Retrieval after 30 days. Set an expiration to delete the data after 2 years.
D. Deploy Amazon EC2 On-Demand Instances to run the batch jobs. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Deep Archive after 30 days. Set an expiration to delete the data after 2 years.

Answer: D

Explanation:

- A: Wrong because Spot cannot be used if jobs cannot be disrupted.

- B: Wrong because storing first in Glacier Instant isn't valid for fresh data.

- C: Wrong because Spot risk disrupts short-lived jobs.

- D: Correct because On-Demand ensures no disruption + S3 tiering reduces cost.

Question 57:
A company needs to design a hybrid network architecture. The company's workloads are currently stored in the AWS Cloud and in on-premises data centers. The workloads require single-digit latencies to communicate. The company uses an AWS Transit Gateway to connect multiple VPCs. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

Options:
A. Establish an AWS Site-to-Site VPN connection to each VPC.
B. Associate an AWS Direct Connect gateway with the transit gateway that is attached to the VPCs.
C. Establish an AWS Site-to-Site VPN connection to an AWS Direct Connect gateway.
D. Establish an AWS Direct Connect connection. Create a transit virtual interface (VIF) to a Direct Connect gateway.
E. Associate AWS Site-to-Site VPN connections with the transit gateway that is attached to the VPCs.

Answer: BD

Explanation:

- A: Wrong because VPN alone doesn't guarantee single-digit latency.

- B: Correct because associating DX gateway with TGW integrates all VPCs.

- C: Wrong because VPN adds latency and not cost-effective.

- D: Correct because Direct Connect provides low-latency dedicated link.

- E: Wrong because VPNs still introduce higher latency.

Question 58:
A global ecommerce company runs its critical workloads on AWS. The workloads use an Amazon RDS for PostgreSQL DB instance that is configured for a Multi-AZ deployment. Customers have reported application timeouts when the company undergoes database failovers. The company needs a resilient solution to reduce failover time. Which solution will meet these requirements?

Options:
A. Create an Amazon RDS Proxy. Assign the proxy to the DB instance.
B. Create a read replica for the DB instance. Move the read traffic to the read replica.
C. Enable Performance Insights. Monitor the CPU load to identify the timeouts.
D. Take regular automatic snapshots. Copy the automatic snapshots to multiple AWS Regions.

Answer: A

Explanation:

- A: Correct because RDS Proxy reduces failover time by managing connections.

- B: Wrong because read replicas don't reduce failover for writes.

- C: Wrong because monitoring CPU doesn't solve failover delay.

- D: Wrong because snapshots don't help with failover speed.

Question 59:
A company has multiple Amazon RDS DB instances that run in a development AWS account. All the instances have tags to identify them as development resources. The company needs the development DB instances to run on a schedule only during business hours. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create an Amazon CloudWatch alarm to identify RDS instances that need to be stopped. Create an AWS Lambda function to start and stop the RDS instances.
B. Create an AWS Trusted Advisor report to identify RDS instances to be started and stopped. Create an AWS Lambda function to start and stop the RDS instances.
C. Create AWS Systems Manager State Manager associations to start and stop the RDS instances.
D. Create an Amazon EventBridge rule that invokes AWS Lambda functions to start and stop the RDS instances.

Answer: C

Explanation:

- A: Wrong because CloudWatch alarms require extra Lambda automation.

- B: Wrong because Trusted Advisor doesn't perform start/stop actions.

- C: Correct because Systems Manager State Manager automates schedules with least effort.

- D: Wrong because EventBridge + Lambda requires more setup.

Question 60:

A consumer survey company has gathered data for several years from a specific geographic region. The company stores this data in an Amazon S3 bucket in an AWS Region. The company has started to share this data with a marketing firm in a new geographic region. The company has granted the firm's AWS account access to the S3 bucket. The company wants to minimize the data transfer costs when the marketing firm requests data from the S3 bucket. Which solution will meet these requirements?

Options:
A. Configure the Requester Pays feature on the company's S3 bucket.
B. Configure S3 Cross-Region Replication (CRR) from the company's S3 bucket to one of the marketing firm's S3 buckets.
C. Configure AWS Resource Access Manager to share the S3 bucket with the marketing firm AWS account.
D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Answer: A

Explanation:

- A: Correct because Requester Pays shifts transfer cost to the requester (marketing firm).

- B: Wrong because CRR doubles storage + cost.

- C: Wrong because RAM shares resources, not data transfer optimization.

- D: Wrong because Intelligent-Tiering is for storage cost, not transfer.

Question 61:
A company uses AWS to host its public ecommerce website. The website uses an AWS Global Accelerator accelerator for traffic from the internet. The Global Accelerator accelerator forwards the traffic to an Application Load Balancer (ALB) that is the entry point for an Auto Scaling group. The company recently identified a DDoS attack on the website. The company needs a solution to mitigate future attacks. Which solution will meet these requirements with the LEAST implementation effort?

Options:
A. Configure an AWS WAF web ACL for the Global Accelerator accelerator to block traffic by using rate-based rules.
B. Configure an AWS Lambda function to read the ALB metrics to block attacks by updating a VPC network ACL.
C. Configure an AWS WAF web ACL on the ALB to block traffic by using rate-based rules.
D. Configure an Amazon CloudFront distribution in front of the Global Accelerator accelerator.

Answer: A

Explanation:

- A: Correct because WAF on Global Accelerator mitigates DDoS quickly with minimal changes.

- B: Wrong because Lambda + NACL updates add complexity.

- C: Wrong because applying WAF at ALB is less effective than at GA edge.

- D: Wrong because adding CloudFront increases complexity without direct need.

Question 62:
A company uses an Amazon DynamoDB table to store data that the company receives from devices. The DynamoDB table supports a customer-facing website to display recent activity on customer devices. The company configured the table with provisioned throughput for writes and reads. The company wants to calculate performance metrics for customer device data on a daily basis. The solution must have minimal effect on the table's provisioned read and write capacity. Which solution will meet these requirements?

Options:
A. Use an Amazon Athena SQL query with the Amazon Athena DynamoDB connector to calculate performance metrics on a recurring schedule.
B. Use an AWS Glue job with the AWS Glue DynamoDB export connector to calculate performance metrics on a recurring schedule.
C. Use an Amazon Redshift COPY command to calculate performance metrics on a recurring schedule.
D. Use an Amazon EMR job with an Apache Hive external table to calculate performance metrics on a recurring schedule.

Answer: B

Explanation:

- A: Wrong because Athena connector queries DynamoDB directly, consuming capacity.

- B: Correct because Glue export connector exports without affecting live table capacity.

- C: Wrong because Redshift COPY requires additional ETL pipeline.

- D: Wrong because EMR introduces overhead compared to Glue export.

Question 63:
A solutions architect is designing the cloud architecture for a new stateless application that will be deployed on AWS. The solutions architect created an Amazon Machine Image (AMI) and launch template for the application. Based on the number of jobs that need to be processed, the processing must run in parallel while adding and removing application Amazon EC2 instances as needed. The application must be loosely coupled. The job items must be durably stored. Which solution will meet these requirements?

Options:
A. Create an Amazon Simple Notification Service (Amazon SNS) topic to send the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on CPU usage.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on network usage.
C. Create an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on the number of items in the SQS queue.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to send the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on the number of messages published to the SNS topic.

Answer: C

Explanation:

- A: Wrong because SNS doesn't provide durable storage.

- B: Wrong because network usage doesn't reflect job backlog.

- C: Correct because SQS ensures durability + scaling on queue length meets parallel job needs.

- D: Wrong because SNS doesn't persist messages.

Question 64:
A global ecommerce company uses a monolithic architecture. The company needs a solution to manage the increasing volume of product data. The solution must be scalable and have a modular service architecture. The company needs to maintain its structured database schemas. The company also needs a storage solution to store product data and product images. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use an Amazon EC2 instance in an Auto Scaling group to deploy a containerized application. Use an Application Load Balancer to distribute web traffic. Use an Amazon RDS DB instance to store product data and product images.
B. Use AWS Lambda functions to manage the existing monolithic application. Use Amazon DynamoDB to store product data and product images. Use Amazon Simple Notification Service (Amazon SNS) for event-driven communication between the Lambda functions.
C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with an Amazon EC2 deployment to deploy a containerized application. Use an Amazon Aurora cluster to store the product data. Use AWS Step Functions to manage workflows. Store the product images in Amazon S3 Glacier Deep Archive.
D. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate to deploy a containerized application. Use Amazon RDS with a Multi-AZ deployment to store the product data. Store the product images in an Amazon S3 bucket.

Answer: D

Explanation:

- A: Wrong because RDS cannot store images efficiently.

- B: Wrong because DynamoDB isn't suitable for structured schema migration.

- C: Wrong because storing images in Glacier DA is unsuitable for frequent access.

- D: Correct because ECS Fargate reduces ops + RDS stores data + S3 for images.

Question 65:
A company is migrating an application from an on-premises environment to AWS. The application will store sensitive data in Amazon S3. The company must encrypt the data before storing the data in Amazon S3. Which solution will meet these requirements?

Options:
A. Encrypt the data by using client-side encryption with customer managed keys.
B. Encrypt the data by using server-side encryption with AWS KMS keys (SSE-KMS).
C. Encrypt the data by using server-side encryption with customer-provided keys (SSE-C).
D. Encrypt the data by using client-side encryption with Amazon S3 managed keys.

Answer: A

Explanation:

- A: Correct because client-side encryption ensures encryption before reaching S3.

- B: Wrong because SSE-KMS is server-side, not client-side pre-encryption.

- C: Wrong because SSE-C requires user to send keys with each request.

- D: Wrong because S3-managed keys aren't available for client-side.

Question 66:
A company wants to create an Amazon EMR cluster that multiple teams will use. The company wants to ensure that each team's big data workloads can access only the AWS services that each team needs to interact with. The company does not want the workloads to have access to Instance Metadata Service Version 2 (IMDSv2) on the cluster's underlying EC2 instances. Which solution will meet these requirements?

Options:
A. Configure interface VPC endpoints for each AWS service that the teams need. Use the required interface VPC endpoints to submit the big data workloads.
B. Create EMR runtime roles. Configure the cluster to use the runtime roles. Use the runtime roles to submit the big data workloads.
C. Create an EC2 IAM instance profile that has the required permissions for each team. Use the instance profile to submit the big data workloads.
D. Create an EMR security configuration that has the EnableApplicationScopedIAMRole option set to false. Use the security configuration to submit the big data workloads.

Answer: B

Explanation:

- A: Wrong because VPC endpoints don't restrict role-level AWS access.

- B: Correct because EMR runtime roles allow scoped permissions per workload.

- C: Wrong because instance profiles expose permissions cluster-wide.

- D: Wrong because disabling scoped IAM roles removes fine-grained control.

Question 67:
A solutions architect is designing an application that helps users fill out and submit registration forms. The solutions architect plans to use a two-tier architecture that includes a web application server tier and a worker tier. The application needs to process submitted forms quickly. The application needs to process each form exactly once. The solution must ensure that no data is lost. Which solution will meet these requirements?

Options:
A. Use an Amazon Simple Queue Service (Amazon SQS) FIFO queue between the web application server tier and the worker tier to store and forward form data.
B. Use an Amazon API Gateway HTTP API between the web application server tier and the worker tier to store and forward form data.
C. Use an Amazon Simple Queue Service (Amazon SQS) standard queue between the web application server tier and the worker tier to store and forward form data.
D. Use an AWS Step Functions workflow. Create a synchronous workflow between the web application server tier and the worker tier that stores and forwards form data.

Answer: A

Explanation:

- A: Correct because FIFO SQS guarantees exactly-once delivery with durability.

- B: Wrong because API Gateway is not a durable store.

- C: Wrong because SQS Standard can deliver duplicates.

- D: Wrong because Step Functions adds complexity and cost.

Question 68:
A finance company uses an on-premises search application to collect streaming data from various producers. The application provides real-time updates to search and visualization features. The company is planning to migrate to AWS and wants to use an AWS native solution. Which solution will meet these requirements?

Options:
A. Use Amazon EC2 instances to ingest and process the data streams to Amazon S3 buckets for storage. Use Amazon Athena to search the data. Use Amazon Managed Grafana to create visualizations.
B. Use Amazon EMR to ingest and process the data streams to Amazon Redshift for storage. Use Amazon Redshift Spectrum to search the data. Use Amazon QuickSight to create visualizations.
C. Use Amazon Elastic Kubernetes Service (Amazon EKS) to ingest and process the data streams to Amazon DynamoDB for storage. Use Amazon CloudWatch to create graphical dashboards to search and visualize the data.
D. Use Amazon Kinesis Data Streams to ingest and process the data streams to Amazon OpenSearch Service. Use OpenSearch Service to search the data. Use Amazon QuickSight to create visualizations.

Answer: D

Explanation:

- A: Wrong because Athena is for querying static S3 data, not real-time.

- B: Wrong because Redshift isn't built for real-time search and visualization.

- C: Wrong because DynamoDB + CloudWatch isn't a search/visualization solution.

- D: Correct because Kinesis + OpenSearch + QuickSight meets real-time ingestion, search, and visualization.

Question 69:
A company currently runs an on-premises application that uses ASP.NET on Linux machines. The application is resource-intensive and serves customers directly. The company wants to modernize the application to .NET. The company wants to run the application on containers and to scale based on Amazon CloudWatch metrics. The company also wants to reduce the time spent on operational maintenance activities. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use AWS App2Container to containerize the application. Use an AWS CloudFormation template to deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
B. Use AWS App2Container to containerize the application. Use an AWS CloudFormation template to deploy the application to Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 instances.
C. Use AWS App Runner to containerize the application. Use App Runner to deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
D. Use AWS App Runner to containerize the application. Use App Runner to deploy the application to Amazon Elastic Kubernetes Service (Amazon EKS) on Amazon EC2 instances.

Answer: A

Explanation:

- A: Correct because App2Container + ECS Fargate reduces ops overhead, supports scaling.

- B: Wrong because ECS on EC2 adds maintenance burden.

- C: Wrong because App Runner is not used with ECS, it's standalone.

- D: Wrong because App Runner doesn't deploy to EKS.

Question 70:
A company is designing a new internal web application in the AWS Cloud. The new application must securely retrieve and store multiple employee usernames and passwords from an AWS managed service. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Store the employee credentials in AWS Systems Manager Parameter Store. Use AWS CloudFormation and the BatchGetSecretValue API to retrieve usernames and passwords from Parameter Store.
B. Store the employee credentials in AWS Secrets Manager. Use AWS CloudFormation and AWS Batch with the BatchGetSecretValue API to retrieve the usernames and passwords from Secrets Manager.
C. Store the employee credentials in AWS Systems Manager Parameter Store. Use AWS CloudFormation and AWS Batch with the BatchGetSecretValue API to retrieve the usernames and passwords from Parameter Store.
D. Store the employee credentials in AWS Secrets Manager. Use AWS CloudFormation and the BatchGetSecretValue API to retrieve the usernames and passwords from Secrets Manager.

Answer: D

Explanation:

- A: Wrong because Parameter Store requires extra setup and doesn't natively rotate secrets.

- B: Wrong because AWS Batch is unrelated for retrieval.

- C: Wrong because Parameter Store + Batch is overcomplicated.

- D: Correct because Secrets Manager securely stores + retrieves with least overhead.

Question 71:
A company that is in the ap-northeast-1 Region has a fleet of thousands of AWS Outposts servers. The company has deployed the servers at remote locations around the world. All the servers regularly download new software versions that consist of 100 files. There is significant latency before all servers run the new software versions. The company must reduce the deployment latency for new software versions. Which solution will meet this requirement with the LEAST operational overhead?

Options:
A. Create an Amazon S3 bucket in ap-northeast-1. Set up an Amazon CloudFront distribution in ap-northeast-1 that includes a CachingDisabled cache policy. Configure the S3 bucket as the origin. Download the software by using signed URLs.
B. Create an Amazon S3 bucket in ap-northeast-1. Create a second S3 bucket in the us-east-1 Region. Configure replication between the buckets. Set up an Amazon CloudFront distribution that uses ap-northeast-1 as the primary origin and us-east-1 as the secondary origin. Download the software by using signed URLs.
C. Create an Amazon S3 bucket in ap-northeast-1. Configure Amazon S3 Transfer Acceleration. Download the software by using the S3 Transfer Acceleration endpoint.
D. Create an Amazon S3 bucket in ap-northeast-1. Set up an Amazon CloudFront distribution. Configure the S3 bucket as the origin. Download the software by using signed URLs.

Answer: C

Explanation:

- A: Wrong because caching disabled CloudFront adds no benefit.

- B: Wrong because replication + dual origins adds complexity.

- C: Correct because S3 Transfer Acceleration reduces latency globally.

- D: Wrong because CloudFront alone won't solve upload/download latency for Outposts.

Question 72:
A company currently runs an on-premises stock trading application by using Microsoft Windows Server. The company wants to migrate the application to the AWS Cloud. The company needs to design a highly available solution that provides low-latency access to block storage across multiple Availability Zones. Which solution will meet these requirements with the LEAST implementation effort?

Options:
A. Configure a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances. Install the application on both cluster nodes. Use Amazon FSx for Windows File Server as shared storage between the two cluster nodes.
B. Configure a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances. Install the application on both cluster nodes. Use Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp3) volumes as storage attached to the EC2 instances. Set up application-level replication to sync data.
C. Deploy the application on Amazon EC2 instances in two Availability Zones. Configure one EC2 instance as active and the second EC2 instance in standby mode. Use an Amazon FSx for NetApp ONTAP Multi-AZ file system to access the data by using iSCSI protocol.
D. Deploy the application on Amazon EC2 instances in two Availability Zones. Configure one EC2 instance as active and the second EC2 instance in standby mode. Use Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io2) volumes with EBS replication.

Answer: A

Explanation:

- A: Correct because FSx for Windows File Server provides multi-AZ, shared storage with minimal setup.

- B: Wrong because manual replication increases complexity.

- C: Wrong because FSx ONTAP is overkill for Windows app migration.

- D: Wrong because EBS replication adds ops overhead.

Question 73:
A company is designing a web application with an internet-facing Application Load Balancer (ALB). The company needs the ALB to receive HTTPS web traffic from the public internet. The ALB must send only HTTPS traffic to the web application servers hosted on the Amazon EC2 instances on port 443. The ALB must perform a health check of the web application servers over HTTPS on port 8443. Which combination of configurations of the security group that is associated with the ALB will meet these requirements? (Choose three.)

Options:
A. Allow HTTPS inbound traffic from 0.0.0.0/0 for port 443.
B. Allow all outbound traffic to 0.0.0.0/0 for port 443.
C. Allow HTTPS outbound traffic to the web application instances for port 443.
D. Allow HTTPS inbound traffic from the web application instances for port 443.
E. Allow HTTPS outbound traffic to the web application instances for the health check on port 8443.
F. Allow HTTPS inbound traffic from the web application instances for the health check on port 8443.

Answer: ACE

Explanation:

- A: Correct because ALB must allow inbound HTTPS from internet on 443.

- B: Wrong because outbound all-traffic not needed.

- C: Correct because ALB needs outbound 443 to send HTTPS to EC2.

- D: Wrong because inbound from EC2 isn't relevant.

- E: Correct because ALB must send health check HTTPS traffic to port 8443.

- F: Wrong because ALB doesn't receive health check traffic from EC2.

Question 74:
A company hosts an application on AWS. The application gives users the ability to upload photos and store the photos in an Amazon S3 bucket. The company wants to use Amazon CloudFront and a custom domain name to upload the photo files to the S3 bucket in the eu-west-1 Region. Which solution will meet these requirements? (Choose two.)

Options:
A. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront.
B. Use AWS Certificate Manager (ACM) to create a public certificate in eu-west-1. Use the certificate in CloudFront.
C. Configure Amazon S3 to allow uploads from CloudFront. Configure S3 Transfer Acceleration.
D. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC).
E. Configure Amazon S3 to allow uploads from CloudFront. Configure an Amazon S3 website endpoint.

Answer: BD

Explanation:

- A: Wrong because CloudFront requires certificate in us-east-1, but uploads require EU cert.

- B: Correct because ACM certificate in eu-west-1 is needed for custom domain.

- C: Wrong because Transfer Acceleration is not needed with CloudFront.

- D: Correct because OAC secures S3 uploads from CloudFront.

- E: Wrong because website endpoints don't support uploads.

Question 75:

A weather forecasting company collects temperature readings from various sensors on a continuous basis. An existing data ingestion process collects the readings and aggregates the readings into larger Apache Parquet files. Then the process encrypts the files by using client-side encryption with KMS managed keys (CSE-KMS). Finally, the process writes the files to an Amazon S3 bucket with separate prefixes for each calendar day. The company wants to run occasional SQL queries on the data to take sample moving averages for a specific calendar day. Which solution will meet these requirements MOST cost-effectively?

Options:

A. Configure Amazon Athena to read the encrypted files. Run SQL queries on the data directly in Amazon S3.
B. Use Amazon S3 Select to run SQL queries on the data directly in Amazon S3.
C. Configure Amazon Redshift to read the encrypted files. Use Redshift Spectrum and Redshift query editor v2 to run SQL queries on the data directly in Amazon S3.
D. Configure Amazon EMR Serverless to read the encrypted files. Use Apache SparkSQL to run SQL queries on the data directly in Amazon S3.

Answer: A

Explanation:

- A: Correct because Athena queries S3 Parquet data directly, cost-effective for occasional queries.

- B: Wrong because S3 Select works at object-level, not dataset-level SQL.

- C: Wrong because Redshift is costly for occasional queries.

- D: Wrong because EMR adds unnecessary overhead.

Question 76:

A company is implementing a new application on AWS. The company will run the application on multiple Amazon EC2 instances across multiple Availability Zones within multiple AWS Regions. The application will be available through the internet. Users will access the application from around the world. The company wants to ensure that each user who accesses the application is sent to the EC2 instances that are closest to the user's location. Which solution will meet these requirements?

Options:

A. Implement an Amazon Route 53 geolocation routing policy. Use an internet-facing Application Load Balancer to distribute the traffic across all Availability Zones within the same Region.
B. Implement an Amazon Route 53 geoproximity routing policy. Use an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region.
C. Implement an Amazon Route 53 multivalue answer routing policy. Use an internet-facing Application Load Balancer to distribute the traffic across all Availability Zones within the same Region.
D. Implement an Amazon Route 53 weighted routing policy. Use an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region.

Answer: B

Explanation:

- A: Wrong because geolocation sends traffic based on country, not closest region.

- B: Correct because geoproximity directs traffic to nearest region, NLB balances within AZs.

- C: Wrong because multivalue answer just returns multiple IPs.

- D: Wrong because weighted splits traffic by ratio, not distance.

Question 77:
A financial services company plans to launch a new application on AWS to handle sensitive financial transactions. The company will deploy the application on Amazon EC2 instances. The company will use Amazon RDS for MySQL as the database. The company's security policies mandate that data must be encrypted at rest and in transit. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit.
B. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure IPsec tunnels for encryption in transit.
C. Implement third-party application-level data encryption before storing data in Amazon RDS for MySQL. Configure AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit.
D. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure a VPN connection to enable private connectivity to encrypt data in transit.

Answer: A

Explanation:

- A: Correct because RDS + KMS handles encryption at rest; ACM covers SSL in transit easily.

- B: Wrong because IPsec tunnels add unnecessary complexity.

- C: Wrong because app-level encryption adds overhead.

- D: Wrong because VPN for encryption in transit is unnecessary with SSL.

Question 78:
A company is migrating its on-premises Oracle database to an Amazon RDS for Oracle database. The company needs to retain data for 90 days to meet regulatory requirements. The company must also be able to restore the database to a specific point in time for up to 14 days. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create Amazon RDS automated backups. Set the retention period to 90 days.
B. Create an Amazon RDS manual snapshot every day. Delete manual snapshots that are older than 90 days.
C. Use the Amazon Aurora Clone feature for Oracle to create a point-in-time restore. Delete clones that are older than 90 days.
D. Create a backup plan that has a retention period of 90 days by using AWS Backup for Amazon RDS.

Answer: D

Explanation:

- A: Wrong because RDS automated backups max retention is 35 days, not 90.

- B: Wrong because manual snapshot management adds overhead.

- C: Wrong because Aurora Clone isn't applicable to Oracle RDS.

- D: Correct because AWS Backup supports longer retention (90 days).

Question 79:
A company is developing a new application that uses a relational database to store user data and application configurations. The company expects the application to have steady user growth. The company expects the database usage to be variable and read-heavy, with occasional writes. The company wants to cost-optimize the database solution. The company wants to use an AWS managed database solution that will provide the necessary performance. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Deploy the database on Amazon RDS. Use Provisioned IOPS SSD storage to ensure consistent performance for read and write operations.
B. Deploy the database on Amazon Aurora Serverless to automatically scale the database capacity based on actual usage to accommodate the workload.
C. Deploy the database on Amazon DynamoDB. Use on-demand capacity mode to automatically scale throughput to accommodate the workload.
D. Deploy the database on Amazon RDS. Use magnetic storage and use read replicas to accommodate the workload.

Answer: B

Explanation:

- A: Wrong because Provisioned IOPS is expensive and not optimized for cost.

- B: Correct because Aurora Serverless scales automatically and handles read-heavy workloads.

- C: Wrong because DynamoDB is NoSQL, not relational.

- D: Wrong because magnetic storage is outdated and slow.

Question 80:
A company hosts its application on several Amazon EC2 instances inside a VPC. The company creates a dedicated Amazon S3 bucket for each customer to store their relevant information in Amazon S3. The company wants to ensure that the application running on EC2 instances can securely access only the S3 buckets that belong to the company's AWS account. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create a gateway endpoint for Amazon S3 that is attached to the VPC. Update the IAM instance profile policy to provide access to only the specific buckets that the application needs.
B. Create a NAT gateway in a public subnet with a security group that allows access to only Amazon S3. Update the route tables to use the NAT Gateway.
C. Create a gateway endpoint for Amazon S3 that is attached to the VPC. Update the IAM instance profile policy with a Deny action and the following condition key.
D. Create a NAT Gateway in a public subnet. Update route tables to use the NAT Gateway. Assign bucket policies for all buckets with a Deny action and the following condition key.

Answer: C

Explanation:

- A: Wrong because IAM policies alone don't prevent cross-account S3.

- B: Wrong because NAT gateway is costly and unnecessary.

- C: Correct because gateway endpoint + Deny condition ensures only internal account S3 access.

- D: Wrong because NAT + bucket policies adds overhead.

Question 81:
A company is building a cloud-based application on AWS that will handle sensitive customer data. The application uses Amazon RDS for the database, Amazon S3 for object storage, and S3 Event Notifications that invoke AWS Lambda for serverless processing. The company uses AWS IAM Identity Center to manage user credentials. The development, testing, and operations teams need secure access to Amazon RDS and Amazon S3 while ensuring the confidentiality of sensitive customer data. The solution must comply with the principle of least privilege. Which solution meets these requirements with the LEAST operational overhead?

Options:
A. Use IAM roles with least privilege to grant all the teams access. Assign IAM roles to each team with customized IAM policies defining specific permission for Amazon RDS and S3 object access based on team responsibilities.
B. Enable IAM Identity Center with an Identity Center directory. Create and configure permission sets with granular access to Amazon RDS and Amazon S3. Assign all the teams to groups that have specific access with the permission sets.
C. Create individual IAM users for each member in all the teams with role-based permissions. Assign the IAM roles with predefined policies for RDS and S3 access to each user based on user needs. Implement IAM Access Analyzer for periodic credential evaluation.
D. Use AWS Organizations to create separate accounts for each team. Implement cross-account IAM roles with least privilege. Grant specific permission for RDS and S3 access based on team roles and responsibilities.

Answer: B

Explanation:

- A: Wrong because IAM role management for all teams adds operational overhead.

- B: Correct because Identity Center + permission sets enforces least privilege with minimal overhead.

- C: Wrong because managing individual IAM users is inefficient.

- D: Wrong because creating separate accounts adds unnecessary complexity.

Question 82:
A company has an Amazon S3 bucket that contains sensitive data files. The company has an application that runs on virtual machines in an on-premises data center. The company currently uses AWS IAM Identity Center. The application requires temporary access to files in the S3 bucket. The company wants to grant the application secure access to the files in the S3 bucket. Which solution will meet these requirements?

Options:
A. Create an S3 bucket policy that permits access to the bucket from the public IP address range of the company's on-premises data center.
B. Use IAM Roles Anywhere to obtain security credentials in IAM Identity Center that grant access to the S3 bucket. Configure the virtual machines to assume the role by using the AWS CLI.
C. Install the AWS CLI on the virtual machine. Configure the AWS CLI with access keys from an IAM user that has access to the bucket.
D. Create an IAM user and policy that grants access to the bucket. Store the access key and secret key for the IAM user in AWS Secrets Manager. Configure the application to retrieve the access key and secret key at startup.

Answer: B

Explanation:

- A: Wrong because IP-based S3 bucket policies are not secure enough.

- B: Correct because IAM Roles Anywhere allows secure temporary access for on-premises workloads.

- C: Wrong because IAM user access keys create long-term credentials.

- D: Wrong because storing IAM user keys in Secrets Manager still uses long-term credentials.

Question 83:
A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services. What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

Options:
A. Create a DX connection in each new account. Route the network traffic to the on-premises servers.
B. Configure VPC endpoints in the DX VPC for all required services. Route the network traffic to the on-premises servers.
C. Create a VPN connection between each new account and the DX VPC. Route the network traffic to the on-premises servers.
D. Configure AWS Transit Gateway between the accounts. Assign DX to the transit gateway and route network traffic to the on-premises servers.

Answer: D

Explanation:

- A: Wrong because separate DX per account is expensive and unnecessary.

- B: Wrong because VPC endpoints are for AWS services, not on-premises services.

- C: Wrong because VPN per account adds management overhead.

- D: Correct because Transit Gateway + DX allows centralized routing with minimal overhead.

Question 84:
A company hosts its main public web application in one AWS Region across multiple Availability Zones. The application uses an Amazon EC2 Auto Scaling group and an Application Load Balancer (ALB). A web development team needs a cost-optimized compute solution to improve the company's ability to serve dynamic content globally to millions of customers. Which solution will meet these requirements?

Options:
A. Create an Amazon CloudFront distribution. Configure the existing ALB as the origin.
B. Use Amazon Route 53 to serve traffic to the ALB and EC2 instances based on the geographic location of each customer.
C. Create an Amazon S3 bucket with public read access enabled. Migrate the web application to the S3 bucket. Configure the S3 bucket for website hosting.
D. Use AWS Direct Connect to directly serve content from the web application to the location of each customer.

Answer: A

Explanation:

- A: Correct because CloudFront caches content globally, reducing latency cost-effectively.

- B: Wrong because Route 53 cannot serve dynamic content.

- C: Wrong because EC2 dynamic app can't just run on S3 static hosting.

- D: Wrong because DX is for private connectivity, not global content delivery.

Question 85:

A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary, with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability. Which storage solution meets these requirements?

Options:

A. Amazon S3 Standard

B. Amazon S3 Intelligent-Tiering

C. Amazon S3 Glacier Deep Archive

D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

- A: Wrong because S3 Standard is costlier for infrequently accessed data.

- B: Correct because Intelligent-Tiering optimizes cost automatically based on usage.

- C: Wrong because Glacier Deep Archive is not for continuous usage.

- D: Wrong because One Zone-IA reduces durability (not multi-AZ).

Question 86:

A company is testing an application that runs on an Amazon EC2 Linux instance. A single 500 GB Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume is attached to the EC2 instance. The company will deploy the application on multiple EC2 instances in an Auto Scaling group. All instances require access to the data that is stored in the EBS volume. The company needs a highly available and resilient solution that does not introduce significant changes to the application's code. Which solution will meet these requirements?

Options:

A. Provision an EC2 instance that uses NFS server software. Attach a single 500 GB gp2 EBS volume to the instance.

B. Provision an Amazon FSx for Windows File Server file system. Configure the file system as an SMB file store within a single Availability Zone.

C. Provision an EC2 instance with two 250 GB Provisioned IOPS SSD EBS volumes.

D. Provision an Amazon Elastic File System (Amazon EFS) file system. Configure the file system to use General Purpose performance mode.

Answer: D

Explanation:

- A: Wrong because single NFS server creates SPOF.

- B: Wrong because FSx Windows File Server is not needed for Linux workloads.

- C: Wrong because splitting into multiple EBS doesn't share across instances.

- D: Correct because EFS is scalable, multi-AZ, and easily shared across EC2.

Question 87:
A company recently launched a new application for its customers. The application runs on multiple Amazon EC2 instances across two Availability Zones. End users use TCP to communicate with the application. The application must be highly available and must automatically scale as the number of users increases. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

Options:
A. Add a Network Load Balancer in front of the EC2 instances.
B. Configure an Auto Scaling group for the EC2 instances.
C. Add an Application Load Balancer in front of the EC2 instances.
D. Manually add more EC2 instances for the application.
E. Add a Gateway Load Balancer in front of the EC2 instances.

Answer: AB

Explanation:

- A: Correct because NLB handles TCP traffic and provides HA.

- B: Correct because Auto Scaling ensures elasticity.

- C: Wrong because ALB is for HTTP/HTTPS, not raw TCP.

- D: Wrong because manual scaling adds ops overhead.

- E: Wrong because GWLB is for security appliances, not apps.

Question 88:
A company is designing the architecture for a new mobile app that uses the AWS Cloud. The company uses organizational units (OUs) in AWS Organizations to manage its accounts. The company wants to tag Amazon EC2 instances with data sensitivity by using values of sensitive and nonsensitive. IAM identities must not be able to delete a tag or create instances without a tag. Which combination of steps will meet these requirements? (Choose two.)

Options:
A. In Organizations, create a new tag policy that specifies the data sensitivity tag key and the required values. Enforce the tag values for the EC2 instances. Attach the tag policy to the appropriate OU.
B. In Organizations, create a new service control policy (SCP) that specifies the data sensitivity tag key and the required tag values. Enforce the tag values for the EC2 instances. Attach the SCP to the appropriate OU.
C. Create a tag policy to deny running instances when a tag key is not specified. Create another tag policy that prevents identities from deleting tags. Attach the tag policies to the appropriate OU.
D. Create a service control policy (SCP) to deny creating instances when a tag key is not specified. Create another SCP that prevents identities from deleting tags. Attach the SCPs to the appropriate OU.
E. Create an AWS Config rule to check if EC2 instances use the data sensitivity tag and the specified values. Configure an AWS Lambda function to delete the resource if a noncompliant resource is found.

Answer: AD

Explanation:

- A: Wrong because tag policies only enforce naming, not blocking creation.

- B: Wrong because SCP can't enforce tag values directly.

- C: Wrong because tag policies don't deny operations.

- D: Correct because SCP enforces creation + prevents tag deletion.

- E: Wrong because Config + Lambda adds unnecessary overhead.

Question 89:
A company runs database workloads on AWS that are the backend for the company's customer portals. The company runs a Multi-AZ database cluster on Amazon RDS for PostgreSQL. The company needs to implement a 30-day backup retention policy. The company currently has both automated RDS backups and manual RDS backups. The company wants to maintain both types of existing RDS backups that are less than 30 days old. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Configure the RDS backup retention policy to 30 days for automated backups by using AWS Backup. Manually delete manual backups that are older than 30 days.
B. Disable RDS automated backups. Delete automated backups and manual backups that are older than 30 days. Configure the RDS backup retention policy to 30 days for automated backups.
C. Configure the RDS backup retention policy to 30 days for automated backups. Manually delete manual backups that are older than 30 days.
D. Disable RDS automated backups. Delete automated backups and manual backups that are older than 30 days automatically by using AWS CloudFormation. Configure the RDS backup retention policy to 30 days for automated backups.

Answer: C

Explanation:

- A: Wrong because AWS Backup is unnecessary for standard RDS backups.

- B: Wrong because disabling automated backups reduces protection.

- C: Correct because retention for automated backups + manual cleanup is simplest.

- D: Wrong because disabling automated backups is unsafe.

Question 90:
A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose. Which storage solution should a solutions architect recommend for use after the migration?

Options:
A. AWS DataSync
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Elastic File System (Amazon EFS)
D. Amazon EMR File System (Amazon EMRFS)

Answer: C

Explanation:

- A: Wrong because DataSync is for data transfer, not continuous storage.

- B: Wrong because EBS can't be shared across multiple instances.

- C: Correct because EFS supports NFS protocol, scalable and multi-AZ.

- D: Wrong because EMRFS is specific to EMR clusters.

Question 91:
A company uses GPS trackers to document the migration patterns of thousands of sea turtles. The trackers check every 5 minutes to see if a turtle has moved more than 100 yards (91.4 meters). If a turtle has moved, its tracker sends the new coordinates to a web application running on three Amazon EC2 instances that are in multiple Availability Zones in one AWS Region. Recently, the web application was overwhelmed while processing an unexpected volume of tracker data. Data was lost with no way to replay the events. A solutions architect must prevent this problem from happening again and needs a solution with the least operational overhead. What should the solutions architect do to meet these requirements?

Options:
A. Create an Amazon S3 bucket to store the data. Configure the application to scan for new data in the bucket for processing.
B. Create an Amazon API Gateway endpoint to handle transmitted location coordinates. Use an AWS Lambda function to process each item concurrently.
C. Create an Amazon Simple Queue Service (Amazon SQS) queue to store the incoming data. Configure the application to poll for new messages for processing.
D. Create an Amazon DynamoDB table to store transmitted location coordinates. Configure the application to query the table for new data for processing. Use TTL to remove data that has been processed.

Answer: C

Explanation:

- A: Wrong because scanning S3 introduces latency.

- B: Wrong because Lambda can struggle with very high concurrency + cost.

- C: Correct because SQS buffers data and prevents loss, ensuring replayability.

- D: Wrong because DynamoDB isn't ideal for event buffering.

Question 92:
A company's software development team needs an Amazon RDS Multi-AZ cluster. The RDS cluster will serve as a backend for a desktop client that is deployed on premises. The desktop client requires direct connectivity to the RDS cluster. The company must give the development team the ability to connect to the cluster by using the client when the team is in the office. Which solution provides the required connectivity MOST securely?

Options:
A. Create a VPC and two public subnets. Create the RDS cluster in the public subnets. Use AWS Site-to-Site VPN with a customer gateway in the company's office.
B. Create a VPC and two private subnets. Create the RDS cluster in the private subnets. Use AWS Site-to-Site VPN with a customer gateway in the company's office.
C. Create a VPC and two private subnets. Create the RDS cluster in the private subnets. Use RDS security groups to allow the company's office IP ranges to access the cluster.
D. Create a VPC and two public subnets. Create the RDS cluster in the public subnets. Create a cluster user for each developer. Use RDS security groups to allow the users to access the cluster.

Answer: B

Explanation:

- A: Wrong because public subnets for RDS are insecure.

- B: Correct because private subnets + VPN ensure secure connectivity.

- C: Wrong because security groups alone don't provide secure connectivity path.

- D: Wrong because public RDS exposure is not secure.

Question 93:
A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances. What should the solutions architect do to reduce the overall data transfer costs?

Options:
A. Place all the EC2 instances in an Auto Scaling group.
B. Place all the EC2 instances in the same AWS Region.
C. Place all the EC2 instances in the same Availability Zone.
D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Answer: C

Explanation:

- A: Wrong because Auto Scaling doesn't affect transfer cost.

- B: Wrong because same Region still incurs inter-AZ transfer costs.

- C: Correct because keeping instances in one AZ avoids cross-AZ charges.

- D: Wrong because private subnets don't reduce costs.

Question 94:
A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days. What should a solutions architect do to meet this requirement with the LEAST operational effort?

Options:
A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS KMS encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
C. Store a file that contains the credentials in an AWS KMS encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
D. Store a file that contains the credentials in an AWS KMS encrypted Amazon S3 bucket. Download the file to the application regularly. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads the new credentials to the file in the S3 bucket.

Answer: A

Explanation:

- A: Correct because Secrets Manager integrates with RDS/Aurora and handles automated rotation.

- B: Wrong because Parameter Store rotation requires custom Lambda.

- C: Wrong because storing in EFS adds complexity.

- D: Wrong because storing in S3 introduces overhead.

Question 95:
A streaming media company is rebuilding its infrastructure to accommodate increasing demand for video content that users consume daily. The company needs to process terabyte-sized videos to block some content in the videos. Video processing can take up to 20 minutes. The company needs a solution that will scale with demand and remain cost-effective. Which solution will meet these requirements?

Options:
A. Use AWS Lambda functions to process videos. Store video metadata in Amazon DynamoDB. Store video content in Amazon S3 Intelligent-Tiering.
B. Use Amazon Elastic Container Service (Amazon ECS) and AWS Fargate to implement microservices to process videos. Store video metadata in Amazon Aurora. Store video content in Amazon S3 Intelligent-Tiering.
C. Use Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) to process videos. Store video content in Amazon S3 Standard. Use Amazon Simple Queue Service (Amazon SQS) for queuing.
D. Deploy a containerized video processing application on Amazon Elastic Kubernetes Service (Amazon EKS) on Amazon EC2. Store video metadata in Amazon RDS in a single Availability Zone. Store video content in Amazon S3 Glacier Deep Archive.

Answer: B

Explanation:

- A: Wrong because Lambda has max timeout (15 mins), not suitable for 20 min jobs.

- B: Correct because ECS + Fargate scales automatically and suits long-running workloads.

- C: Wrong because EC2 + ASG works but adds more ops overhead.

- D: Wrong because Glacier Deep Archive is not suitable for active video storage.

Question 96:
A company runs an on-premises application on a Kubernetes cluster. The company recently added millions of new customers. The company's existing on-premises infrastructure is unable to handle the large number of new customers. The company needs to migrate the on-premises application to the AWS Cloud. The company will migrate to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The company does not want to manage the underlying compute infrastructure for the new architecture on AWS. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use a self-managed node to supply compute capacity. Deploy the application to the new EKS cluster.
B. Use managed node groups to supply compute capacity. Deploy the application to the new EKS cluster.
C. Use AWS Fargate to supply compute capacity. Create a Fargate profile. Use the Fargate profile to deploy the application.
D. Use managed node groups with Karpenter to supply compute capacity. Deploy the application to the new EKS cluster.

Answer: C

Explanation:

- A: Wrong because self-managed nodes increase ops burden.

- B: Wrong because managed node groups still require EC2 management.

- C: Correct because Fargate provides serverless compute for EKS pods.

- D: Wrong because Karpenter still requires managing nodes.

Question 97:
A company is launching a new application that requires a structured database to store user profiles, application settings, and transactional data. The database must be scalable with application traffic and must offer backups. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Deploy a self-managed database on Amazon EC2 instances by using open source software. Use Spot Instances for cost optimization. Configure automated backups to Amazon S3.
B. Use Amazon RDS. Use on-demand capacity mode for the database with General Purpose SSD storage. Configure automatic backups with a retention period of 7 days.
C. Use Amazon Aurora Serverless for the database. Use serverless capacity scaling. Configure automated backups to Amazon S3.
D. Deploy a self-managed NoSQL database on Amazon EC2 instances. Use Reserved Instances for cost optimization. Configure automated backups directly to Amazon S3 Glacier Flexible Retrieval.

Answer: C

Explanation:

- A: Wrong because self-managed adds heavy ops overhead.

- B: Wrong because RDS on-demand doesn't scale as efficiently as Aurora Serverless.

- C: Correct because Aurora Serverless scales automatically and provides backups.

- D: Wrong because NoSQL doesn't meet relational database requirement.

Question 98:
A company runs its legacy web application on AWS. The web application server runs on an Amazon EC2 instance in the public subnet of a VPC. The web application server collects images from customers and stores the image files in a locally attached Amazon Elastic Block Store (Amazon EBS) volume. The image files are uploaded every night to an Amazon S3 bucket for backup. A solutions architect discovers that the image files are being uploaded to Amazon S3 through the public endpoint. The solutions architect needs to ensure that traffic to Amazon S3 does not use the public endpoint. Which solution will meet these requirements?

Options:
A. Create a gateway VPC endpoint for the S3 bucket that has the necessary permissions for the VPC. Configure the subnet route table to use the gateway VPC endpoint.
B. Move the S3 bucket inside the VPC. Configure the subnet route table to access the S3 bucket through private IP addresses.
C. Create an Amazon S3 access point for the Amazon EC2 instance inside the VPC. Configure the web application to upload by using the Amazon S3 access point.
D. Configure an AWS Direct Connect connection between the VPC that has the Amazon EC2 instance and Amazon S3 to provide a dedicated network path.

Answer: A

Explanation:

- A: Correct because gateway VPC endpoint allows private S3 access.

- B: Wrong because S3 is a regional service, not inside a VPC.

- C: Wrong because access point doesn't solve public endpoint issue.

- D: Wrong because Direct Connect is unnecessary for S3 traffic.

Question 99:
A company is creating a prototype of an ecommerce website on AWS. The website consists of an Application Load Balancer, an Auto Scaling group of Amazon EC2 instances for web servers, and an Amazon RDS for MySQL DB instance that runs with the Single-AZ configuration. The website is slow to respond during searches of the product catalog. The product catalog is a group of tables in the MySQL database that the company does not update frequently. A solutions architect has determined that the CPU utilization on the DB instance is high when product catalog searches occur. What should the solutions architect recommend to improve the performance of the website during searches of the product catalog?

Options:
A. Migrate the product catalog to an Amazon Redshift database. Use the COPY command to load the product catalog tables.
B. Implement an Amazon ElastiCache for Redis cluster to cache the product catalog. Use lazy loading to populate the cache.
C. Add an additional scaling policy to the Auto Scaling group to launch additional EC2 instances when database response is slow.
D. Turn on the Multi-AZ configuration for the DB instance. Configure the EC2 instances to throttle the product catalog queries that are sent to the database.

Answer: B

Explanation:

- A: Wrong because Redshift is for analytics, not OLTP searches.

- B: Correct because caching catalog searches reduces DB load.

- C: Wrong because scaling EC2 doesn't reduce DB bottleneck.

- D: Wrong because Multi-AZ adds HA, not performance.

Question 100:
A company currently stores 5 TB of data in on-premises block storage systems. The company's current storage solution provides limited space for additional data. The company runs applications on premises that must be able to retrieve frequently accessed data with low latency. The company requires a cloud-based storage solution. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A. Use Amazon S3 File Gateway. Integrate S3 File Gateway with the on-premises applications to store and directly retrieve files by using the SMB file system.
B. Use an AWS Storage Gateway Volume Gateway with cached volumes as iSCSI targets.
C. Use an AWS Storage Gateway Volume Gateway with stored volumes as iSCSI targets.
D. Use an AWS Storage Gateway Tape Gateway. Integrate Tape Gateway with the on-premises applications to store virtual tapes in Amazon S3.

Answer: B

Explanation:

- A: Wrong because File Gateway works at file level, not block storage.

- B: Correct because Volume Gateway cached volumes keep hot data locally and store rest in S3.

- C: Wrong because stored volumes require local storage scaling.

- D: Wrong because Tape Gateway is for backups, not block storage.

Question: 101
A company is developing a marketing communications service that targets mobile app users. The company needs to send confirmation messages with Short Message Service (SMS) to its users. The users must be able to reply to the SMS messages. The company must store the responses for a year for analysis.
What should a solutions architect do to meet these requirements?

Options:
A. Create an Amazon Connect contact flow to send the SMS messages. Use AWS Lambda to process the responses.
B. Build an Amazon Pinpoint journey. Configure Amazon Pinpoint to send events to an Amazon Kinesis data stream for analysis and archiving.
C. Use Amazon Simple Queue Service (Amazon SQS) to distribute the SMS messages. Use AWS Lambda to process the responses.
D. Create an Amazon Simple Notification Service (Amazon SNS) FIFO topic. Subscribe an Amazon Kinesis data stream to the SNS topic for analysis and archiving.

Answer: B

Explanation:

- A: Incorrect. Amazon Connect is for contact center solutions, not SMS reply management.

- B: Correct. Pinpoint supports two-way SMS and integrates with Kinesis for event storage and analytics.

- C: Incorrect. SQS is not designed for SMS messaging.

- D: Incorrect. SNS FIFO topics do not handle SMS replies and archiving directly.

Question: 102
A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
B. Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.
C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.
D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Answer: B

Explanation:

- A: Incorrect. SSE-S3 uses AWS-managed keys but does not provide customer control over rotation.

- B: Correct. KMS customer-managed keys with auto-rotation meet encryption + annual rotation with low effort.

- C: Incorrect. Manual rotation adds operational overhead.

- D: Incorrect. Imported key material does not support automatic rotation.

Question: 103
The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.
As the company expands, customers report that their meeting invitations are taking longer to arrive.
What should a solutions architect recommend to resolve this issue?

Options:
A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
C. Add an Amazon CloudFront distribution. Set the origin as the web application that accepts the appointment requests.
D. Add an Auto Scaling group for the application that sends meeting invitations. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Answer: D

Explanation:

- A: Incorrect. DAX improves read latency, not write/processing delays.

- B: Incorrect. API Gateway doesn't address scaling for backend processing.

- C: Incorrect. CloudFront caches content but doesn't help backend queue processing.

- D: Correct. Scaling the consumer app based on queue depth ensures timely processing.

Question: 104

An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.
The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead.
Which solution will meet these requirements?

Options:

A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.
B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3. Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.
C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register the S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.
D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Answer: C

Explanation:

- A: Incorrect. Moving all data to RDS adds cost and complexity, not ideal for analytics.

- B: Incorrect. Manual copying increases operational overhead and lacks fine-grained permissions.

- C: Correct. Lake Formation integrates S3 + RDS, provides unified data lake and fine-grained access control.

- D: Incorrect. Redshift requires ETL and overhead to load/manage data.

Question: 105

A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.

The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.

Which solution will meet these requirements?

Options:

A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.

B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer. Upload website content by using an SFTP client.

C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using the AWS CLI.

D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Answer: C

Explanation:

- A: Incorrect. Lightsail adds server management overhead.

- B: Incorrect. EC2 + ALB is not cost-effective for static content.

- C: Correct. S3 with OAI + CloudFront is cost-effective, resilient, and secure.

- D: Incorrect. Public S3 bucket for hosting introduces security risks.

Question: 106

A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

Options:

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.

B. Configure AWS CloudTrail with an Amazon Simple Notification Service (Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the CreateImage API call. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.

D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Answer: C

Explanation:

- A: Incorrect. Lambda polling CloudTrail adds more ops overhead.

- B: Incorrect. CloudTrail + Athena adds unnecessary complexity.

- C: Correct. EventBridge natively captures API events and can trigger SNS.

- D: Incorrect. SQS adds extra step and complexity compared to direct EventBridge → SNS.

Question: 107

A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.

The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.

What should a solutions architect do to address this issue without impacting existing users?

Options:

A. Add throttling on the API Gateway with server-side throttling limits.

B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.

C. Create a secondary index in DynamoDB for the table with the user requests.

D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Answer: D

Explanation:

- A: Incorrect. Throttling reduces traffic but still loses requests.

- B: Incorrect. DAX improves reads, not write buffering.

- C: Incorrect. Secondary index does not reduce write traffic load.

- D: Correct. SQS buffers writes, ensuring no data loss under heavy traffic.

Question: 108

A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

Options:

A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

D. Use the AWS provided, publicly available ip-ranges.json file to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Answer: A

Explanation:

- A: Correct. Interface VPC endpoint ensures private connectivity with resource policy restricting IAM role.

- B: Incorrect. Gateway endpoints don't support security groups.

- C: Incorrect. Manually routing by IP is not supported.

- D: Incorrect. Using ip-ranges.json is unreliable and unnecessary.

Question: 109
A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.
What should the solutions architect do to ensure that the architecture supports distributed session data management?

Options:
A. Use Amazon ElastiCache to manage and store session data.
B. Use session affinity (sticky sessions) of the ALB to manage session data.
C. Use Session Manager from AWS Systems Manager to manage the session.
D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

Answer: A

Explanation:

- A: Correct. ElastiCache provides centralized session storage across instances.

- B: Incorrect. Sticky sessions reduce availability and scalability.

- C: Incorrect. Session Manager is for system access, not app sessions.

- D: Incorrect. STS tokens are for authentication, not session storage.

Question: 110
A company offers a food delivery service that is growing rapidly. Because of the growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes the following:
• A group of Amazon EC2 instances that run in an Amazon EC2 Auto Scaling group to collect orders from the application
• Another group of EC2 instances that run in an Amazon EC2 Auto Scaling group to fulfill orders
The order collection process occurs quickly, but the order fulfillment process can take longer. Data must not be lost because of a scaling event.
A solutions architect must ensure that the order collection process and the order fulfillment process can both scale properly during peak traffic hours. The solution must optimize utilization of the company's AWS resources.
Which solution meets these requirements?

Options:
A. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure each Auto Scaling group's minimum capacity according to peak workload values.
B. Use Amazon CloudWatch metrics to monitor the CPU of each instance in the Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic that creates additional Auto Scaling groups on demand.
C. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Scale the Auto Scaling groups based on notifications that the queues send.
D. Provision two Amazon Simple Queue Service (Amazon SQS) queues: one for order collection and another for order fulfillment. Configure the EC2 instances to poll their respective queue. Create a metric based on a backlog per instance calculation. Scale the Auto Scaling groups based on this metric.

Answer: D

Explanation:

- A: Incorrect. Hardcoding peak capacity wastes resources.

- B: Incorrect. Spawning new Auto Scaling groups adds unnecessary complexity.

- C: Incorrect. Notifications alone aren't optimal for scaling.

- D: Correct. Backlog per instance metric provides efficient scaling of consumers.

Question: 111

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of "application" and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.
Which solution meets these requirements?

Options:
A. Use AWS CloudTrail to generate a list of resources with the application tag.
B. Use the AWS CLI to query each service across all Regions to report the tagged components.
C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

Answer: D

Explanation:

- A: Incorrect. CloudTrail tracks API calls, not resource tag inventories.

- B: Incorrect. Querying via CLI across all Regions is time-consuming.

- C: Incorrect. Logs Insights doesn't provide global tagged resource reports.

- D: Correct. Tag Editor provides a global view of resources by tag quickly.

Question: 112

A company needs to export its database once a day to Amazon S3 for other teams to access. The exported object size varies between 2 GB and 5 GB. The S3 access pattern for the data is variable and changes rapidly. The data must be immediately available and must remain accessible for up to 3 months. The company needs the most cost-effective solution that will not increase retrieval time.
Which S3 storage class should the company use to meet these requirements?

Options:
A. S3 Intelligent-Tiering
B. S3 Glacier Instant Retrieval
C. S3 Standard
D. S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: A

Explanation:

- A: Correct. Intelligent-Tiering adapts storage class automatically, minimizing cost with immediate access.

- B: Incorrect. Glacier Instant Retrieval is costlier for frequent unpredictable access.

- C: Incorrect. S3 Standard works but costs more.

- D: Incorrect. S3 Standard-IA charges retrieval fees and is not optimal for unpredictable usage.

Question: 113

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment.

What should a solutions architect recommend to meet these requirements?

Options:

A. Configure AWS WAF rules and associate them with the ALB.
B. Deploy the application using Amazon S3 with public hosting enabled.
C. Deploy AWS Shield Advanced and add the ALB as a protected resource.
D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

Answer: A

Explanation:

- A: Correct. AWS WAF protects ALBs from SQL injection and XSS.

- B: Incorrect. S3 static hosting doesn't meet the ALB protection requirement.

- C: Incorrect. Shield Advanced is for DDoS, not app-level attacks.

- D: Incorrect. Third-party firewall adds more ops overhead.

Question: 114

A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.

Which solution will meet these requirements with the LEAST development effort?

Options:

A. Create an Amazon EMR cluster with Apache Spark installed. Write a Spark application to transform the data. Use EMR File System (EMRFS) to write files to the transformed data bucket.
B. Create an AWS Glue crawler to discover the data. Create an AWS Glue extract, transform, and load (ETL) job to transform the data. Specify the transformed data bucket in the output step.
C. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucket. Use the job definition to submit a job. Specify an array job as the job type.
D. Create an AWS Lambda function to transform the data and output the data to the transformed data bucket. Configure an event notification for the S3 bucket. Specify the Lambda function as the destination for the event notification.

Answer: B

Explanation:

- A: Incorrect. EMR requires custom coding and more ops.

- B: Correct. Glue ETL is serverless and low overhead for format conversion.

- C: Incorrect. Batch requires job setup and scripting effort.

- D: Incorrect. Lambda isn't suited for large-scale .csv → Parquet conversions.

Question: 115

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.
What should a solutions architect do to migrate and store the data at the LOWEST cost?

Options:
A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

Answer: A

Explanation:

- A: Correct. Snowball accelerates bulk migration within a month and Glacier Deep Archive is cheapest.

- B: Incorrect. VPN transfer over internet is too slow for 700 TB.

- C: Incorrect. Provisioning Direct Connect is time-consuming and costly.

- D: Incorrect. DataSync over 500 Mbps link can't migrate 700 TB in 1 month.

Question: 116

A company has a serverless website with millions of objects in an Amazon S3 bucket. The company uses the S3 bucket as the origin for an Amazon CloudFront distribution. The company did not set encryption on the S3 bucket before the objects were loaded. A solutions architect needs to enable encryption for all existing objects and for all objects that are added to the S3 bucket in the future.
Which solution will meet these requirements with the LEAST amount of effort?

Options:
A. Create a new S3 bucket. Turn on the default encryption settings for the new S3 bucket. Download all existing objects to temporary local storage. Upload the objects to the new S3 bucket.
B. Turn on the default encryption settings for the S3 bucket. Use the S3 Inventory feature to create a .csv file that lists the unencrypted objects. Run an S3 Batch Operations job that uses the copy command to encrypt those objects.
C. Create a new encryption key by using AWS Key Management Service (AWS KMS). Change the settings on the S3 bucket to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Turn on versioning for the S3 bucket.
D. Navigate to Amazon S3 in the AWS Management Console. Browse the S3 bucket's objects. Sort by the encryption field. Select each unencrypted object. Use the Modify button to apply default encryption settings to every unencrypted object in the S3 bucket.

Answer: B

Explanation:

- A: Incorrect. Manual download/upload is inefficient.

- B: Correct. S3 Batch Operations with Inventory automates encryption for existing + future objects.

- C: Incorrect. SSE-KMS adds cost but doesn't auto-encrypt past objects.

- D: Incorrect. Manual encryption object-by-object is impractical.

Question: 117
A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy. What should a solutions architect do to meet these requirements?

Options:
A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

Answer: A

Explanation:

- A: Correct. Active-passive with Aurora Replica in another Region meets 30-min RTO/RPO.

- B: Incorrect. Active-active is unnecessary and costly.

- C: Incorrect. Restoring from snapshot increases downtime beyond 30 minutes.

- D: Incorrect. AWS Backup restore is too slow for 30-min downtime tolerance.

Question: 118

A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Choose two.)

Options:

A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.

B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.

C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.

D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.

E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Answer: AE

Explanation:

- A: Correct. Security group must allow inbound HTTPS.

- B: Incorrect. SGs use source for inbound, not destination.

- C: Incorrect. ACL must also allow outbound ephemeral ports.

- D: Incorrect. Outbound 443 isn't correct for responses.

- E: Correct. NACL needs inbound 443 and outbound ephemeral range.

Question: 119

A company's application is having performance issues. The application is stateful and needs to complete in-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 instance family. As traffic increased, the application performance degraded. Users are reporting delays when the users attempt to access the application.

Which solution will resolve these issues in the MOST operationally efficient way?

Options:

A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group. Make the changes by using the AWS Management Console.

B. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary.

C. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.

D. Modify the CloudFormation templates. Replace the EC2 instances with R5 EC2 instances. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Answer: D

Explanation:

- A: Incorrect. T3 burstable instances are not suitable for sustained in-memory workloads.

- B: Incorrect. Manual scaling adds overhead.

- C: Incorrect. Built-in metrics don't include memory/latency; CloudWatch agent is required.

- D: Correct. R5 optimized for memory + CloudWatch agent for detailed monitoring is best.

Question: 120

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable; several hours can pass without receiving a single request. The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

Options:
A. An AWS Glue job
B. An AWS Lambda function
C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)
D. A containerized service hosted in Amazon ECS with Amazon EC2

Answer: B

Explanation:

- A: Incorrect. Glue is for batch ETL, not suitable for real-time API triggers.

- B: Correct. Lambda scales to zero, serverless, and cost-effective for sporadic workloads.

- C: Incorrect. EKS adds ops overhead for low traffic APIs.

- D: Incorrect. ECS with EC2 requires managing compute resources.

Question: 121

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years. The log files will be analyzed by a reporting tool that must be able to access all the files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

Options:

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon EC2 instance store
D. Amazon S3

Answer: D

Explanation:

- A: Incorrect. EBS volumes are tied to instances and costly for 7-year retention.

- B: Incorrect. EFS is costlier than S3 for long-term storage.

- C: Incorrect. Instance store is ephemeral, unsuitable for compliance retention.

- D: Correct. S3 provides durable, concurrent access, low cost, ideal for 7-year logs.

Question: 122

A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account.

How should a solutions architect grant this access to the vendor?

Options:

A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
C. Create an IAM group in the company's account. Add the tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
D. Create a new identity provider by choosing "AWS account" as the provider type in the IAM console. Supply the vendor's AWS account ID and user name. Attach the appropriate IAM policies to the new provider for the permissions that the vendor requires.

Answer: A

Explanation:

- A: Correct. Cross-account IAM role with trust policy allows vendor to assume securely.

- B: Incorrect. IAM user creates direct credentials, less secure.

- C: Incorrect. Groups cannot include users from another AWS account.

- D: Incorrect. No such provider type for AWS account.

Question: 123
A company has deployed a Java Spring Boot application as a pod that runs on Amazon Elastic Kubernetes Service (Amazon EKS) in private subnets. The application needs to write data to an Amazon DynamoDB table. A solutions architect must ensure that the application can interact with the DynamoDB table without exposing traffic to the internet.
Which combination of steps should the solutions architect take to accomplish this goal? (Choose two.)

Options:
A. Attach an IAM role that has sufficient privileges to the EKS pod.
B. Attach an IAM user that has sufficient privileges to the EKS pod.
C. Allow outbound connectivity to the DynamoDB table through the private subnets' network ACLs.
D. Create a VPC endpoint for DynamoDB.
E. Embed the access keys in the Java Spring Boot code.

Answer: AD

Explanation:

- A: Correct. IAM roles for service accounts give pods secure access.

- B: Incorrect. IAM user credentials not recommended.

- C: Incorrect. NACLs are not sufficient without private endpoint.

- D: Correct. VPC endpoint ensures private DynamoDB access.

- E: Incorrect. Hardcoding keys is insecure.

Question: 124
A company recently migrated its web application to AWS by rehosting the application on Amazon EC2 instances in a single AWS Region. The company wants to redesign its application architecture to be highly available and fault tolerant. Traffic must reach all running EC2 instances randomly.
Which combination of steps should the company take to meet these requirements? (Choose two.)

Options:
A. Create an Amazon Route 53 failover routing policy.
B. Create an Amazon Route 53 weighted routing policy.
C. Create an Amazon Route 53 multivalue answer routing policy.
D. Launch three EC2 instances: two instances in one Availability Zone and one instance in another Availability Zone.
E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

Answer: CE

Explanation:

- A: Incorrect. Failover routing is for DR scenarios.

- B: Incorrect. Weighted routing not required for equal load.

- C: Correct. Multivalue routing randomly distributes DNS responses.

- D: Incorrect. Two + one AZ setup doesn't balance evenly.

- E: Correct. Two AZs with equal capacity provides high availability.

Question: 125

A media company collects and analyzes user activity data on premises. The company wants to migrate this capability to AWS. The user activity data store will continue to grow and will be petabytes in size. The company needs to build a highly available data ingestion solution that facilitates on-demand analytics of existing data and new data with SQL.

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

Options:

A. Send activity data to an Amazon Kinesis data stream. Configure the stream to deliver the data to an Amazon S3 bucket.

B. Send activity data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Redshift cluster.

C. Place activity data in an Amazon S3 bucket. Configure Amazon S3 to run an AWS Lambda function on the data as the data arrives in the S3 bucket.

D. Create an ingestion service on Amazon EC2 instances that are spread across multiple Availability Zones. Configure the service to forward data to an Amazon RDS Multi-AZ database.

Answer: B

Explanation:

- A: Incorrect. Kinesis Data Streams requires consumer management.

- B: Correct. Firehose → Redshift automates ingestion, low ops.

- C: Incorrect. Lambda triggers aren't scalable for petabytes.

- D: Incorrect. EC2-based ingestion has high overhead.

Question: 126

A company collects data from thousands of remote devices by using a RESTful web services application that runs on an Amazon EC2 instance. The EC2 instance receives the raw data, transforms the raw data, and stores all the data in an Amazon S3 bucket. The number of remote devices will increase into the millions soon. The company needs a highly scalable solution that minimizes operational overhead.

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

Options:

A. Use AWS Glue to process the raw data in Amazon S3.

B. Use Amazon Route 53 to route traffic to different EC2 instances.

C. Add more EC2 instances to accommodate the increasing amount of incoming data.

D. Send the raw data to Amazon Simple Queue Service (Amazon SQS). Use EC2 instances to process the data.

E. Use Amazon API Gateway to send the raw data to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to use the data stream as a source to deliver the data to Amazon S3.

Answer: AE

Explanation:

- A: Correct. Glue processes raw → structured efficiently.

- B: Incorrect. Route 53 routing doesn't scale ingestion.

- C: Incorrect. Adding EC2 doesn't scale to millions.

- D: Incorrect. SQS adds complexity without solving ingest scaling.

- E: Correct. API Gateway + Kinesis Firehose scales ingest seamlessly.

Question: 127

A company needs to retain its AWS CloudTrail logs for 3 years. The company is enforcing CloudTrail across a set of AWS accounts by using AWS Organizations from the parent account. The CloudTrail target S3 bucket is configured with S3 Versioning enabled. An S3 Lifecycle policy is in place to delete current objects after 3 years. After the fourth year of use of the S3 bucket, the S3 bucket metrics show that the number of objects has continued to rise. However, the number of new CloudTrail logs that are delivered to the S3 bucket has remained consistent. Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

Options:

A. Configure the organization's centralized CloudTrail trail to expire objects after 3 years.
B. Configure the S3 Lifecycle policy to delete previous versions as well as current versions.
C. Create an AWS Lambda function to enumerate and delete objects from Amazon S3 that are older than 3 years.
D. Configure the parent account as the owner of all objects that are delivered to the S3 bucket.

Answer: B

Explanation:

- A: Incorrect. CloudTrail doesn't control object expiration.

- B: Correct. S3 Lifecycle must target both current and previous versions.

- C: Incorrect. Lambda adds unnecessary overhead.

- D: Incorrect. Object ownership doesn't solve version retention.

Question: 128

A company has an API that receives real-time data from a fleet of monitoring devices. The API stores this data in an Amazon RDS DB instance for later analysis. The amount of data that the monitoring devices send to the API fluctuates. During periods of heavy traffic, the API often returns timeout errors.

After an inspection of the logs, the company determines that the database is not capable of processing the volume of write traffic that comes from the API. A solutions architect must minimize the number of connections to the database and must ensure that data is not lost during periods of heavy traffic.

Which solution will meet these requirements?

Options:

A. Increase the size of the DB instance to an instance type that has more available memory.
B. Modify the DB instance to be a Multi-AZ DB instance. Configure the application to write to all active RDS DB instances.
C. Modify the API to write incoming data to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function that Amazon SQS invokes to write data from the queue to the database.
D. Modify the API to write incoming data to an Amazon Simple Notification Service (Amazon SNS) topic. Use an AWS Lambda function that Amazon SNS invokes to write data from the topic to the database.

Answer: C

Explanation:

- A: Incorrect. Scaling up may not solve spikes effectively.

- B: Incorrect. Multi-AZ improves HA, not write throughput.

- C: Correct. SQS buffers writes, Lambda reduces DB connections.

- D: Incorrect. SNS is for pub/sub, not buffering large writes.

Question: 129
A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.
Which solution meets these requirements?

Options:
A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Answer: A

Explanation:

- A: Correct. Aurora Serverless MySQL provides autoscaling + durability with low ops.

- B: Incorrect. PostgreSQL is not MySQL-compatible.

- C: Incorrect. Larger EC2 creates scaling limits.

- D: Incorrect. Auto Scaling for DBs isn't effective for stateful MySQL.

Question: 130
A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available, fault tolerant, and automatically scalable.
What should the solutions architect recommend?

Options:
A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Answer: C

Explanation:

- A: Incorrect. Single AZ doesn't provide HA.

- B: Incorrect. NAT instances require ops management.

- C: Correct. NAT gateways in multiple AZs provide HA, fault tolerance, scalability.

- D: Incorrect. Spot Instances unsuitable for NAT reliability.

Question: 131
An application runs on an Amazon EC2 instance that has an Elastic IP address in VPC A. The application requires access to a database in VPC B. Both VPCs are in the same AWS account. Which solution will provide the required access MOST securely?

Options:
A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
B. Configure a VPC peering connection between VPC A and VPC B.
C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Answer: B

Explanation:

- A: Incorrect. Allowing via public IP is less secure.

- B: Correct. VPC peering allows secure private connectivity.

- C: Incorrect. Making DB public violates security best practices.

- D: Incorrect. Proxy adds latency and unnecessary resources.

Question: 132
A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

Options:
A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.
B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Answer: C

Explanation:

- A: Incorrect. Application Insights does not detect SSH/RDP traffic.

- B: Incorrect. SSM role is for management, not traffic monitoring.

- C: Correct. Flow logs + metric filters detect RDP/SSH and send alerts.

- D: Incorrect. State-change doesn't cover network connections.

Question: 133
A solutions architect has created a new AWS account and must secure AWS account root user access.
Which combination of actions will accomplish this? (Choose two.)

Options:
A. Ensure the root user uses a strong password.
B. Enable multi-factor authentication to the root user.
C. Store root user access keys in an encrypted Amazon S3 bucket.
D. Add the root user to a group containing administrative permissions.
E. Apply the required permissions to the root user with an inline policy document.

Answer: AB

Explanation:

- A: Correct. Strong password reduces risk.

- B: Correct. MFA is critical for securing root user.

- C: Incorrect. Best practice is to delete root access keys.

- D: Incorrect. Root cannot be added to groups.

- E: Incorrect. Root already has full permissions.

Question: 134
A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.
Which solution will meet these requirements?

Options:
A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS). Attach the KMS keys to the ALB to encrypt data in transit.

Answer: C

Explanation:

- A: Incorrect. ACM is for TLS, KMS for storage encryption. Mix is wrong.

- B: Incorrect. Root account doesn't enable account-wide encryption toggle.

- C: Correct. KMS encrypts storage at rest, ACM provides TLS for ALB.

- D: Incorrect. BitLocker not required; AWS-native solutions preferred.

Question: 135
A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.
What should a solutions architect recommend?

Options:
A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Answer: C

Explanation:

- A: Incorrect. DataSync is for file transfer, not database migration.

- B: Incorrect. Missing schema conversion required for Oracle → Postgres.

- C: Correct. SCT + DMS with CDC ensures ongoing sync during phased migration.

- D: Incorrect. Compute optimized instance not necessary, memory optimized is.

Question: 136

A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.
Which solution meets these requirements?

Options:

A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.

B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.

C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.

D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.

Answer: D

Explanation:

- A: Incorrect. Too much redesign (Lambda, DynamoDB).

- B: Incorrect. Multi read replicas are not needed; Multi-AZ RDS suffices.

- C: Incorrect. Memory optimized EC2 DB lacks HA.

- D: Correct. Elastic Beanstalk for scaling front/app layers + RDS Multi-AZ + S3 = HA with minimal changes.

Question: 137

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.
Which solution will meet these requirements?

Options:

A. Set up a VPC peering connection between VPC-A and VPC-B.

B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.

C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.

D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Answer: A

Explanation:

- A: Correct. VPC peering supports secure private comms across accounts.

- B: Incorrect. VPC endpoints connect to AWS services, not EC2 instances.

- C: Incorrect. Virtual private gateway is for VPN/Direct Connect, not EC2 access.

- D: Incorrect. Private VIF is for DX, not VPC-to-VPC.

Question: 138
A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.
What should a solutions architect do to meet this requirement MOST cost-effectively?

Options:
A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Answer: C

Explanation:

- A: Incorrect. Cost Explorer doesn't send automated alerts.

- B: Incorrect. Same as A, no alerting ability.

- C: Correct. AWS Budgets is designed for cost alerts per service/account.

- D: Incorrect. Overly complex setup for simple budget alerts.

Question: 139
A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.
Which solution will deploy the function in the MOST operationally efficient way?

Options:
A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
C. Create an Amazon CloudFront distribution. Deploy the function to Integrate IAM authentication logic into the function.
D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Answer: A

Explanation:

- A: Correct. API Gateway supports HTTPS + IAM auth + Lambda integration.

- B: Incorrect. Lambda function URLs do not support IAM authentication.

- C: Incorrect. doesn't directly integrate with IAM.

- D: Incorrect. CloudFront Functions lack IAM auth support.

Question: 140

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

Options:

A. Host the visualization tool on premises and query the data warehouse directly over the internet.

B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.

C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.

D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Answer: D

Explanation:

- A: Incorrect. Internet transfer costs apply.

- B: Incorrect. Internet egress still charged.

- C: Incorrect. DX between on-premises + AWS still involves large data transfer.

- D: Correct. Hosting viz tool in AWS same Region eliminates egress cost.

Question: 141
An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.
Which solution will meet these requirements with the LEAST amount of operational overhead?

Options:
A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Answer: C

Explanation:

- A: Incorrect. EC2-based DBs need manual replication.

- B: Incorrect. Multi-AZ provides HA within one Region only.

- C: Correct. Cross-Region read replica provides continuous sync and availability.

- D: Incorrect. Snapshots are periodic, not continuous.

Question: 142
A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.
Which policy should be used to meet this requirement?

Options:
A. Simple routing policy
B. Latency routing policy
C. Multivalue routing policy
D. Geolocation routing policy

Answer: C

Explanation:

- A: Incorrect. Simple routing returns only one record.

- B: Incorrect. Latency routing directs to lowest-latency Region.

- C: Correct. Multivalue returns multiple IPs for healthy resources.

- D: Incorrect. Geolocation directs based on user's location.

Question: 143

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

Options:

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.

C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.

D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Answer: A

Explanation:

- A: Correct. File gateway caches S3 locally, minimizing latency.

- B: Incorrect. DataSync is for migrations, not real-time file serving.

- C: Incorrect. Volume gateway is for iSCSI block storage, not file sharing.

- D: Incorrect. EFS is for VPC access, not on-premises clinics.

Question: 144

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

Options:

A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.

B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Answer: C

Explanation:

- A: Incorrect. HA not achieved with single AZ.

- B: Incorrect. Read replica in same AZ doesn't add HA.

- C: Correct. Aurora Multi-AZ + ALB + ASG provides HA and scalability.

- D: Incorrect. Running DB on EC2 is less resilient.

Question: 145

A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

Options:

A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.

B. Change the ALB balancing algorithm to least outstanding requests.

C. Reduce the size of the EC2 instances in both environments.

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.

Answer: A

Explanation:

- A: Correct. Development can run on single instance to save cost.

- B: Incorrect. Changing algorithm doesn't save cost.

- C: Incorrect. Reducing size affects performance in prod too.

- D: Incorrect. Reducing max count doesn't guarantee cost savings.

Question: 146

A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

Options:

A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.

B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.

D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Answer: D

Explanation:

- A: Incorrect. NAT is for outbound traffic, not inbound requests.

- B: Incorrect. Making instances public breaks design.

- C: Incorrect. Outbound rules don't fix inbound traffic.

- D: Correct. ALB must be in public subnets and forward traffic privately.

Question: 147
A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.
Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

Options:
A. Enable binlog replication on the RDS primary node.
B. Choose a failover priority for the source DB instance.
C. Allow long-running transactions to complete on the source DB instance.
D. Create a global table and specify the AWS Regions where the table will be available.
E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Answer: CE

Explanation:

- A: Incorrect. Binlog replication is managed by RDS automatically.

- B: Incorrect. Failover priority applies to Multi-AZ, not replicas.

- C: Correct. Long transactions must finish before replica creation.

- D: Incorrect. DynamoDB global tables, irrelevant here.

- E: Correct. Backups must be enabled for replica creation.

Question: 148
A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed. Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.
What should a solutions architect do to meet these requirements?

Options:
A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.
D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Answer: D

Explanation:

- A: Incorrect. Adding one copy isn't scalable.

- B: Incorrect. VPC endpoint reduces data transfer cost, not CPU utilization.

- C: Incorrect. Vertical scaling has limits.

- D: Correct. SQS decouples workload, ASG scales with demand.

Question: 149
A company is implementing a shared storage solution for a media application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.
Which AWS solution meets these requirements?

Options:
A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

Answer: D

Explanation:

- A: Incorrect. Volume gateway exposes block storage, not SMB.

- B: Incorrect. Tape gateway is for backups.

- C: Incorrect. EC2 self-managed is not fully managed.

- D: Correct. FSx for Windows File Server provides SMB fully managed.

Question: 150
A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.
What should a solutions architect do to meet these requirements when configuring the logs?

Options:
A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Answer: D

Explanation:

- A: Incorrect. CloudWatch Logs storage cost is higher long-term.

- B: Incorrect. Kinesis is not for retention of logs.

- C: Incorrect. CloudTrail tracks API calls, not VPC Flow Logs.

- D: Correct. S3 + lifecycle to IA optimizes cost after 90 days.

Question: 151
An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.
What should a solutions architect do to meet these requirements?

Options:
A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Answer: B

Explanation:

- A: Incorrect. Private subnet cannot directly use IGW.

- B: Correct. NAT gateway in a public subnet allows private subnet EC2 outbound traffic.

- C: Incorrect. NAT instance in same private subnet won't work.

- D: Incorrect. Misconfigured; IGW doesn't route private subnet directly.

Question: 152
A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.
The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.
Which solution meets these requirements?

Options:
A. Amazon Elastic File System (Amazon EFS)
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon S3 Glacier Deep Archive
D. AWS Backup

Answer: A

Explanation:

- A: Correct. EFS is a managed, redundant, shared file system.

- B: Incorrect. EBS volumes attach to a single instance.

- C: Incorrect. Glacier is archival, not simultaneous access.

- D: Incorrect. Backup is for snapshots, not live access.

Question: 153

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group. A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

Options:
A. Deleting IAM users
B. Deleting directories
C. Deleting Amazon EC2 instances
D. Deleting logs from Amazon CloudWatch Logs

Answer: C

Explanation:

- A: Incorrect. No mention of IAM admin permissions.

- B: Incorrect. Directory deletion not tied to policies.

- C: Correct. Policies allow EC2 delete action.

- D: Incorrect. CloudWatch delete not mentioned.

Question: 154

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.
What should a solutions architect do to correct this issue?

Options:
A. Create security group rules using the instance ID as the source or destination.
B. Create security group rules using the security group ID as the source or destination.
C. Create security group rules using the VPC CIDR blocks as the source or destination.
D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B

Explanation:

- A: Incorrect. SGs don't support instance ID rules.

- B: Correct. Use SG IDs for least privilege between tiers.

- C: Incorrect. CIDR block is too broad.

- D: Incorrect. Subnet rules are still broad.

Question: 155

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

Options:

A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.

B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request. Use Lambda to query the database, call the payment service, and pass in the order information.

C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS, retrieve the message, and process the order.

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Answer: D

Explanation:

- A: Incorrect. Kinesis Firehose isn't designed for deduplication.

- B: Incorrect. CloudTrail rules aren't for workflow control.

- C: Incorrect. SNS isn't FIFO, can cause duplicates.

- D: Correct. SQS FIFO ensures exactly-once order processing.

Question: 156

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

Options:

A. Enable a read-only bucket ACL.
B. Enable versioning on the bucket.
C. Attach an IAM policy to the bucket.
D. Enable MFA Delete on the bucket.
E. Encrypt the bucket using AWS KMS.

Answer: BD

Explanation:

- A: Incorrect. Read-only ACL prevents updates.

- B: Correct. Versioning preserves history of docs.

- C: Incorrect. IAM policy alone doesn't prevent deletion.

- D: Correct. MFA Delete prevents accidental deletions.

- E: Incorrect. Encryption ensures security, not version control.

Question: 157
A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.
How should the company move the data to Amazon S3 to meet these requirements?

Options:
A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.
D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Answer: A

Explanation:

- A: Correct. Metric streams + Kinesis Firehose → S3 = serverless and efficient.

- B: Incorrect. EMR is overkill.

- C: Incorrect. Scheduled rule misses real-time updates.

- D: Incorrect. Bootstrap delays instance launch.

Question: 158
A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Answer: D

Explanation:

- A: Incorrect. Lambda not suited for 1 GB file conversions.

- B: Incorrect. Spark + Lambda is overcomplicated.

- C: Incorrect. Athena queries aren't for file format conversion.

- D: Correct. Glue ETL jobs scale for big file format conversion.

Question: 159
A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.
Which solution should a solutions architect recommend to meet these requirements?

Options:
A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Answer: A

Explanation:

- A: Correct. AWS Backup provides retention policies, scheduling, restores.

- B: Incorrect. Snapshot retention isn't directly supported.

- C: Incorrect. CloudWatch Logs not for full backups.

- D: Incorrect. DMS is replication, not backup management.

Question: 160

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

Options:

A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.

B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.

C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.

D. Join the file system to the Active Directory to restrict access.

Answer: D

Explanation:

- A: Incorrect. AD Connector is for AWS IAM integration, not SMB file access.

- B: Incorrect. Tags do not enforce AD group permissions.

- C: Incorrect. Service-linked roles manage services, not AD file permissions.

- D: Correct. FSx integrates with on-prem AD to enforce group-based access.

Question: 161

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

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

Options:

A. Configure Amazon CloudFront to cache multiple versions of the content.

B. Configure a host header in a Network Load Balancer to forward traffic to different instances.

C. Configure a function to send specific objects to users based on the User-Agent header.

D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.

E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Answer: AC

Explanation:

- A: Correct. CloudFront caches different content versions.

- B: Incorrect. Host headers do not detect user device types.

- C: Correct. inspects headers to serve device-specific content.

- D: Incorrect. Global Accelerator does not perform content routing.

- E: Incorrect. Path-based routing does not handle device type differentiation.

Question: 162

A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.
The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.
Which solution will meet these requirements MOST cost-effectively?

Options:

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Answer: A

Explanation:

- A: Correct. VPC peering is cost-effective and allows direct communication.

- B: Incorrect. Transit VPC is complex and costly for this case.

- C: Incorrect. Security groups don't apply to VPC peering connections.

- D: Incorrect. Transit VPC adds unnecessary overhead.

Question: 163

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

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

Options:

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.

B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.

C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.

D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.

E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: AD

Explanation:

- A: Correct. ECS is a managed container orchestration service.

- B: Incorrect. Self-managing Kubernetes adds complexity.

- C: Incorrect. EC2 launch type requires instance management.

- D: Correct. ECS with Fargate removes infra management and scales easily.

- E: Incorrect. Managing Kubernetes nodes adds ops overhead.

Question: 164

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

Options:

A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.

B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.

C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Answer: D

Explanation:

- A: Incorrect. Simple routing doesn't handle multiple healthy/unhealthy gracefully.

- B: Incorrect. Failover is for primary/secondary, not 10 EC2 instances.

- C: Incorrect. CloudFront isn't meant for direct EC2 health-based routing.

- D: Correct. ALB health checks + Route 53 ensures only healthy targets get traffic.

Question: 165
A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.
Which solution meets these requirements and is MOST secure?

Options:
A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer: C

Explanation:

- A: Incorrect. EC2 in public subnet reduces security.

- B: Incorrect. CloudFront origin must be ALB, not private EC2.

- C: Correct. EC2 in private subnets + ALB + CloudFront = secure + fast delivery.

- D: Incorrect. Public EC2 increases attack surface.

Question: 166
A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.
Which solution meets these requirements?

Options:
A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Answer: A

Explanation:

- A: Correct. Global Accelerator provides low-latency routing + health checks.

- B: Incorrect. CloudFront adds caching but doesn't solve health-based failover.

- C: Incorrect. S3 isn't relevant here.

- D: Incorrect. DAX addresses caching, not traffic routing.

Question: 167
A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.
D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Answer: D

Explanation:

- A: Incorrect. Lambda adds extra overhead; Firehose can do delivery.

- B: Incorrect. EMR adds high ops complexity.

- C: Incorrect. EMR is overkill for analytics.

- D: Correct. Firehose → S3 (Parquet) + KDA = minimal overhead, scalable.

Question: 168

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture.
What should a solutions architect do to meet these requirements?

Options:
A. Use Amazon ElastiCache in front of the database.
B. Use RDS Proxy between the application and the database.
C. Migrate the application from EC2 instances to AWS Lambda.
D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Answer: B

Explanation:

- A: Incorrect. ElastiCache can help, but caching logic needs code changes.

- B: Correct. RDS Proxy improves connection management with minimal change.

- C: Incorrect. Moving to Lambda requires major redesign.

- D: Incorrect. DynamoDB requires schema and app changes.

Question: 169

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.
What should the solutions architect recommend?

Options:
A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
C. Create a read replica of the primary database and have the business analysts run their queries.
D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer: C

Explanation:

- A: Incorrect. DynamoDB requires re-architecting.

- B: Incorrect. ElastiCache isn't suited for ad-hoc queries.

- C: Correct. RDS read replicas offload queries from primary with minimal changes.

- D: Incorrect. Redshift requires ETL and changes.

Question: 170

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.
Which solution meets these requirements?

Options:

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Answer: A

Explanation:

- A: Correct. Client-side ensures data encrypted before reaching S3.

- B: Incorrect. Server-side encrypts after upload, not before.

- C: Incorrect. SSE-S3 enforces encryption, but only server-side.

- D: Incorrect. Default SSE-KMS is still server-side only.

Question: 171

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.
What should the solutions architect do to meet these requirements?

Options:

A. Increase the minimum capacity for the Auto Scaling group.
B. Increase the maximum capacity for the Auto Scaling group.
C. Configure scheduled scaling to scale up to the desired compute level.
D. Change the scaling policy to add more EC2 instances during each scaling operation.

Answer: C

Explanation:

- A: Incorrect. Raising min keeps unnecessary capacity all day.

- B: Incorrect. Max alone won't pre-scale.

- C: Correct. Scheduled scaling matches predictable workload.

- D: Incorrect. Still reactive, not proactive.

Question: 172

A company serves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency for users that are located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

What should a solutions architect do to meet these requirements?

Options:

A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.

B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.

C. Create an Amazon API Gateway API that is integrated with the ALB. Configure the API to use the HTTP integration type. Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.

D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Answer: B

Explanation:

- A: Incorrect. App is dynamic, not just static.

- B: Correct. CloudFront caches responses from ALB globally, reducing latency.

- C: Incorrect. API Gateway not suited for web content.

- D: Incorrect. Manual caching infra is complex.

Question: 173
A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.
Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

Options:
A. Use an Amazon Aurora global database with a pilot light deployment.
B. Use an Amazon Aurora global database with a warm standby deployment.
C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment.
D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment.

Answer: B

Explanation:

- A: Incorrect. Pilot light means infra is mostly off, slower RTO.

- B: Correct. Warm standby + Aurora global DB ensures low latency + fast recovery.

- C: Incorrect. Multi-AZ is within a Region, not cross-Region.

- D: Incorrect. RDS Multi-AZ doesn't support global DR.

Question: 174
A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.
Which solution will meet these requirements in the MOST operationally efficient way?

Options:
A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.
B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Answer: B

Explanation:

- A: Incorrect. Lambda + custom scripts add ops burden.

- B: Correct. AMIs + CloudFormation automates DR infra quickly.

- C: Incorrect. Keeping instances running wastes resources.

- D: Incorrect. AZ failover doesn't cover Region-level disaster.

Question: 175
A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning. How should the scaling be changed to address the staff complaints and keep costs to a minimum?

Options:
A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Answer: C

Explanation:

- A: Incorrect. Always scaling to 20 may waste cost.

- B: Incorrect. Step scaling reacts slower than target tracking.

- C: Correct. Target tracking ensures faster scaling based on load.

- D: Incorrect. Fixing min/max at 20 is costly.

Question: 176
A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.
What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

Options:
A. Configure storage Auto Scaling on the RDS for Oracle instance.
B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
C. Configure an alarm on the RDS for Oracle instance for low free storage space.
D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Answer: AD

Explanation:

- A: Correct. Storage Auto Scaling handles unpredictable DB growth.

- B: Incorrect. Aurora migration unnecessary here.

- C: Incorrect. Alarm only notifies, no scaling.

- D: Correct. CPU metric helps Auto Scaling respond to load.

- E: Incorrect. Memory metric less reliable than CPU usage.

Question: 177

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.
Which storage solution is MOST cost-effective?

Options:
A. Use AWS Storage Gateway for files to store and process the video content.
B. Use AWS Storage Gateway for volumes to store and process the video content.
C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

Answer: D

Explanation:

- A: Incorrect. Storage Gateway is for hybrid setups.

- B: Incorrect. Volumes don't solve cost issues.

- C: Incorrect. EFS still costly for bulk data.

- D: Correct. S3 is cheap storage, EBS used temporarily for processing.

Question: 178

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

Options:
A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.
C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Answer: BE

Explanation:

- A: Incorrect. Redshift is OLAP, not hierarchical/noSQL.

- B: Correct. DynamoDB is fast and supports hierarchy modeling.

- C: Incorrect. Lambda unnecessary here.

- D: Incorrect. Athena/QuickSight are BI, not OLTP.

- E: Correct. Macie + EventBridge + SNS identifies sensitive data.

Question: 179

A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.
Which solution will meet these requirements?

Options:
A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.
C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.
D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Answer: A

Explanation:

- A: Correct. AWS Backup handles scheduling, retention, lifecycle.

- B: Incorrect. DynamoDB backups don't transition to Glacier directly.

- C: Incorrect. Custom scripts add unnecessary overhead.

- D: Incorrect. CLI commands lack lifecycle transition support.

Question: 180
A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.
What should a solutions architect do to meet these requirements?

Options:
A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Answer: B

Explanation:

- A: Incorrect. Glue is for ETL, not visualization.

- B: Correct. Athena queries + QuickSight visualizations = best fit.

- C: Incorrect. DynamoDB not suited for CloudFront logs.

- D: Incorrect. DynamoDB not involved here.

Question: 181
A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.
Which solution meets these requirements?

Options:
A. Enable a Multi-AZ deployment for the DB instance.
B. Enable auto scaling for the DB instance in one Availability Zone.
C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Answer: A

Explanation:

- A: Correct. Multi-AZ provides synchronous replication with RPO <1s.

- B: Incorrect. Auto scaling doesn't address RPO.

- C: Incorrect. Replicas are asynchronous.

- D: Incorrect. DMS CDC not intended for RPO SLA.

Question: 182

A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.
Which solution will meet these requirements?

Options:
A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.
B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.
D. Configure the security group for the ALB to allow any TCP traffic on any port.

Answer: B

Explanation:

- A: Incorrect. Exposes EC2 directly to internet.

- B: Correct. SG referencing ALB SG restricts access precisely.

- C: Incorrect. Public subnets expose EC2.

- D: Incorrect. Allows all traffic, insecure.

Question: 183

A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.
The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.
Which solution will meet these requirements?

Options:
A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Answer: D

Explanation:

- A: Incorrect. Apps aren't serverless-ready.

- B: Incorrect. FSx File Gateway is for hybrid, not EC2 app integration.

- C: Incorrect. SQS not file-level exchange.

- D: Correct. FSx for NetApp ONTAP supports both NFS + SMB for shared use.

Question: 184
As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.
Which solution meets these requirements?

Options:
A. Run a query with Amazon Athena to generate the report.
B. Create a report in Cost Explorer and download the report.
C. Access the bill details from the billing dashboard and download the bill.
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

Explanation:

- A: Incorrect. Athena isn't needed for billing data.

- B: Correct. Cost Explorer provides per-user breakdown.

- C: Incorrect. Billing dashboard is less granular.

- D: Incorrect. Budgets notify, not report.

Question: 185
A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.
B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).
C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Answer: B

Explanation:

- A: Incorrect. ECS is too heavy for 100 visits/month.

- B: Correct. Serverless + SES is minimal cost.

- C: Incorrect. Lightsail adds unnecessary resources.

- D: Incorrect. Running EC2 24/7 wastes cost.

Question: 186
A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.
A solutions architect needs to implement a solution that displays the updates on the website. Which solution will meet these requirements?

Options:
A. Add an Application Load Balancer.
B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
C. Invalidate the CloudFront cache.
D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Answer: C

Explanation:

- A: Incorrect. ALB unrelated to cache.

- B: Incorrect. ElastiCache doesn't fix CloudFront caching.

- C: Correct. CloudFront invalidation ensures new files show.

- D: Incorrect. SSL cert unrelated.

Question: 187
A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.
How should a solutions architect design the architecture to meet these requirements?

Options:
A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Answer: B

Explanation:

- A: Incorrect. FSx File Gateway is hybrid, not for intra-cloud sharing.

- B: Correct. FSx for Windows supports SMB + integrates with SQL Server on EC2.

- C: Incorrect. EFS is NFS, not compatible with Windows workloads.

- D: Incorrect. EBS volumes can't be shared across EC2 instances.

Question: 188
A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application.
What should a solutions architect do to meet these requirements?

Options:
A. Create an Amazon S3 Standard bucket with access to the web servers.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Answer: C

Explanation:

- A: Incorrect. S3 not POSIX compliant.

- B: Incorrect. CloudFront caches static files, not shared file system.

- C: Correct. EFS provides shared NFS storage across Linux servers.

- D: Incorrect. EBS cannot attach to multiple instances simultaneously.

Question: 189
A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.
Which solution will meet these requirements in the MOST secure manner?

Options:
A. Apply an S3 bucket policy that grants read access to the S3 bucket.
B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Answer: B

Explanation:

- A: Incorrect. Bucket policy not needed when same account + role available.

- B: Correct. Role with least privilege is most secure.

- C: Incorrect. Hardcoding credentials is insecure.

- D: Incorrect. Grants overly broad access.

Question: 190
A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.
Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

Options:
A. Dedicated Instances only
B. On-Demand Instances only
C. A mix of On-Demand Instances and Spot Instances
D. A mix of On-Demand Instances and Reserved Instances

Answer: C

Explanation:

- A: Incorrect. Dedicated instances are costly.

- B: Incorrect. On-Demand only is flexible but not cost optimized.

- C: Correct. On-Demand for baseline, Spot for cost savings.

- D: Incorrect. Reserved Instances require long-term commitment.

Question: 191

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

Options:

A. Signed cookies
B. Signed URLs
C. AWS AppSync
D. JSON Web Token (JWT)
E. AWS Secrets Manager

Answer: AB

Explanation:

- A: Correct. Signed cookies support clients that handle cookies.

- B: Correct. Signed URLs support clients without cookies.

- C: Incorrect. AppSync is unrelated.

- D: Incorrect. JWT not directly tied to CloudFront/S3 access.

- E: Incorrect. Secrets Manager stores secrets, not distribution access.

Question: 192

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

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

Options:

A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Answer: AB

Explanation:

- A: Correct. Kinesis + Firehose + KDA + Athena supports SQL queries.

- B: Correct. MSK + Glue ETL + Athena works with minimal changes.

- C: Incorrect. DMS not designed for streaming.

- D: Incorrect. RDS query editor cannot query S3.

- E: Incorrect. Same as D.

Question: 193

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.
Which solution meets these requirements?

Options:

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Answer: D

Explanation:

- A: Incorrect. Snowball is for bulk transfers, not ongoing backups.

- B: Incorrect. Snowball Edge is temporary transfer, not continuous.

- C: Incorrect. Cached mode stores most data in AWS, not locally.

- D: Correct. Stored mode keeps primary data local + backups in AWS.

Question: 194

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

Options:

A. Create a private hosted zone by using Amazon Route 53.

B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.

C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.

D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

Answer: B

Explanation:

- A: Incorrect. Route 53 doesn't solve private S3 access.

- B: Correct. Gateway VPC endpoint enables private access to S3.

- C: Incorrect. NAT traverses internet gateway, not private.

- D: Incorrect. VPN unnecessary within AWS.

Question: 195

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

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

Options:

A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.

B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.

C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.

D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Answer: B

Explanation:

- A: Incorrect. Proxy app adds operational burden.

- B: Correct. S3 Object Lambda removes PII dynamically with minimal ops.

- C: Incorrect. Maintaining multiple datasets adds cost and ops.

- D: Incorrect. Same as C with DynamoDB overhead.

Question: 196

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

Options:

A. 10.0.1.0/32

B. 192.168.0.0/24

C. 192.168.1.0/32

D. 10.0.1.0/24

Answer: D

Explanation:

- A: Incorrect. /32 allows only one IP.

- B: Incorrect. Same CIDR conflicts with peering.

- C: Incorrect. /32 too small.

- D: Correct. 10.0.1.0/24 non-overlapping valid CIDR.

Question: 197

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%. A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

Options:

A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.

B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.

C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.

D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

Answer: B

Explanation:

- A: Incorrect. Lambda termination is inefficient.

- B: Correct. Auto Scaling with target tracking balances cost + performance.

- C: Incorrect. No scaling policy defined.

- D: Incorrect. Manual intervention needed.

Question: 198
A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.
The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.
Which solution will make the application highly available?

Options:
A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.

Answer: C

Explanation:

- A: Incorrect. RDS needs Multi-AZ, not multiple connections.

- B: Incorrect. Subnets cannot span AZs.

- C: Correct. ASG distributes across AZs + RDS Multi-AZ ensures DB HA.

- D: Incorrect. Subnets don't extend across AZs.

Question: 199

A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data. Which solution will meet the performance requirements?

Options:

A. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to ALL. Import the raw data into the file system. Mount the file system on the EC2 instances.

B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.

C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.

D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Answer: B

Explanation:

- A: Incorrect. NetApp ONTAP not optimal for HPC workloads.

- B: Correct. FSx for Lustre SSD delivers sub-ms latency + >6 GBps throughput.

- C: Incorrect. HDD not performant enough.

- D: Incorrect. ONTAP not designed for HPC at this scale.

Question: 200

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.
What should a solutions architect do to meet these requirements MOST cost-effectively?

Options:

A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.

B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.

C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.

D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

Answer: C

Explanation:

- A: Incorrect. Spot is not reliable for 24/7 apps.

- B: Incorrect. On-Demand RDS costs more for long-term.

- C: Correct. Reserved EC2 + Reserved Aurora = cost savings + scalability.

- D: Incorrect. On-Demand EC2 less cost-efficient.

Question 201:
A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
B.Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the Aurora read replicate to a new Aurora PostgreSQL DB cluster.
C.Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
D.Use the pg_dump utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.

Answer: B

Explanation:

- Aurora read replica ensures near real-time replication with minimal downtime before cutover.

- Option A snapshot method incurs downtime during restore.

- Option C S3 import doesn't keep data in sync.

- Option D pg_dump/restore is manual and time-consuming.

Question 202:
A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster. What should the solutions architect do to meet this requirement with the LEAST amount of effort?

Options:
A.Take a snapshot of the EBS storage that is attached to each EC2 instance. Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
B.Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.
C.Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances.
D.Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.

Answer: C

Explanation:

- AWS Backup centralizes backups across EC2/EBS with least effort and supports mass restore.

- Option A snapshots + CloudFormation is manual and heavy.

- Option B Elastic Beanstalk not meant for disaster recovery of EC2 fleets.

- Option D Lambda automation adds custom overhead.

Question 203:
A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in parallel. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Use the AWS Step Functions Map state in Inline mode to process the data in parallel.
B.Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.
C.Use AWS Glue to process the data in parallel.
D.Use several AWS Lambda functions to process the data in parallel.

Answer: B

Explanation:

- Step Functions Distributed Map scales to thousands of parallel executions automatically.

- Option A Inline Map limits concurrency.

- Option C Glue is good for ETL, not scalable event-driven parallelism.

- Option D Lambda individually managed is less efficient.

Question 204:
A company will migrate 10 PB of data to Amazon S3 in 6 weeks. The current data center has a 500 Mbps uplink to the internet. Other on-premises applications share the uplink. The company can use 80% of the internet bandwidth for this one-time migration task. Which solution will meet these requirements?

Options:
A.Configure AWS DataSync to migrate the data to Amazon S3 and to automatically verify the data.
B.Use rsync to transfer the data directly to Amazon S3.
C.Use the AWS CLI and multiple copy processes to send the data directly to Amazon S3.
D.Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

Answer: D

Explanation:

- Snowball devices handle PB-scale transfers offline efficiently.

- Option A DataSync over 500 Mbps cannot complete 10 PB in 6 weeks.

- Option B rsync is internet-based, not feasible.

- Option C AWS CLI copy still bottlenecked by bandwidth.

Question 205:
A company has several on-premises Internet Small Computer Systems Interface (iSCSI) network storage servers. The company wants to reduce the number of these servers by moving to the AWS Cloud. A solutions architect must provide low-latency access to frequently used data and reduce the dependency on on-premises servers with a minimal number of infrastructure changes. Which solution will meet these requirements?

Options:
A.Deploy an Amazon S3 File Gateway.
B.Deploy Amazon Elastic Block Store (Amazon EBS) storage with backups to Amazon S3.
C.Deploy an AWS Storage Gateway volume gateway that is configured with stored volumes.
D.Deploy an AWS Storage Gateway volume gateway that is configured with cached volumes.

Answer: D

Explanation:

- Cached volumes keep frequently used data locally with cloud storage as primary, reducing dependency.

- Option A S3 File Gateway is for file/NFS/SMB, not iSCSI block.

- Option B EBS is cloud-native, not directly accessible from on-prem.

- Option C stored volumes rely heavily on local storage, not reducing dependency.

Question 206:
A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days. Which solution meets these requirements MOST cost-effectively?

Options:
A.Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
B.Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
C.Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
D.Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Answer: B

Explanation:

- S3 Standard → S3 Standard-IA optimizes cost for infrequent access while keeping durability and availability.

- Option A Glacier retrieval takes hours, not suitable.

- Option C One Zone-IA less durable, not best for critical data.

- Option D Intelligent-Tiering adds monitoring cost, less efficient for known access patterns.

Question 207:
A company has migrated a two-tier application from its on-premises data center to the AWS Cloud. The data tier is a Multi-AZ deployment of Amazon RDS for Oracle with 12 TB of General Purpose SSD Amazon Elastic Block Store (Amazon EBS) storage. The application is designed to process and store documents in the database as binary large objects (blobs) with an average document size of 6 MB. The database size has grown over time, reducing the performance and increasing the cost of storage. The company must improve the database performance and needs a solution that is highly available and resilient. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.
B.Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.
C.Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.
D.Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Answer: C

Explanation:

- Storing blobs in S3 offloads large objects and reduces DB load, while metadata stays in DB.

- Option A Magnetic storage worsens performance.

- Option B Provisioned IOPS costly and doesn't solve blob problem.

- Option D DynamoDB migration breaks relational model.

Question 208:
A company has an application that serves clients that are deployed in more than 20,000 retail storefront locations around the world. The application consists of backend web services that are exposed over HTTPS on port 443. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The retail locations communicate with the web application over the public internet. The company allows each retail location to register the IP address that the retail location has been allocated by its local ISP. The company's security team recommends to increase the security of the application endpoint by restricting access to only the IP addresses registered by the retail locations. What should a solutions architect do to meet these requirements?

Options:
A.Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.
B.Deploy AWS Firewall Manager to manage the ALB. Configure firewall rules to restrict traffic to the ALB. Modify the firewall rules to include the registered IP addresses.
C.Store the IP addresses in an Amazon DynamoDB table. Configure an AWS Lambda authorization function on the ALB to validate that incoming requests are from the registered IP addresses.
D.Configure the network ACL on the subnet that contains the public interface of the ALB. Update the ingress rules on the network ACL with entries for each of the registered IP addresses.

Answer: A

Explanation:

- WAF web ACL with IP rule sets is easiest and scales for large IP list.

- Option B Firewall Manager is for managing multiple accounts, adds overhead.

- Option C Lambda auth increases latency and complexity.

- Option D NACLs limited rule capacity, not practical for 20,000+ IPs

Question 209:
A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an IAM role that includes permissions to access Lake Formation tables.
B.Create data filters to implement row-level security and cell-level security.
C.Create an AWS Lambda function that removes sensitive information before Lake Formation ingests the data.
D.Create an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables.

Answer: B

Explanation:

- Lake Formation supports row-level and cell-level security natively with low operational effort.

- Option A IAM role does not provide fine-grained filtering.

- Option C Lambda preprocessing adds custom overhead.

- Option D periodic cleanup is reactive, not secure.

Question 210:

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances. Which solution will meet these requirements?

Options:

A.Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.

B.Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.

C.Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.

D.Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Answer: B

Explanation:

- Gateway VPC endpoint ensures private access to S3, Direct Connect provides secure connectivity to on-prem.

- Option A interface endpoint is not for S3.

- Option C Transit Gateway doesn't provide S3 access.

- Option D NAT/proxy still uses internet.

Question 211:

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances. The third-party vendor has received many 503 Service Unavailable errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests. Which design should a solutions architect recommend to provide a more scalable solution?

Options:

A.Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.

B.Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.

C.Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.

D.Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Answer: A

Explanation:

- Kinesis Data Streams buffers spikes and scales horizontally with Lambda processing.

- Option B throttles vendor but doesn't solve scaling.

- Option C SNS doesn't support streaming ingest well.

- Option D ECS still suffers from scaling delays.

Question 212:
A company has an application that runs on Amazon EC2 instances in a private subnet. The application needs to process sensitive information from an Amazon S3 bucket. The application must not use the internet to connect to the S3 bucket. Which solution will meet these requirements?

Options:
A.Configure an internet gateway. Update the S3 bucket policy to allow access from the internet gateway. Update the application to use the new internet gateway.
B.Configure a VPN connection. Update the S3 bucket policy to allow access from the VPN connection. Update the application to use the new VPN connection.
C.Configure a NAT gateway. Update the S3 bucket policy to allow access from the NAT gateway. Update the application to use the new NAT gateway.
D.Configure a VPC endpoint. Update the S3 bucket policy to allow access from the VPC endpoint. Update the application to use the new VPC endpoint.

Answer: D

Explanation:

- VPC endpoint allows private connectivity from VPC to S3 without internet.

- Option A internet gateway violates requirement.

- Option B VPN is unnecessary.

- Option C NAT still routes over internet.

Question 213:
A company uses Amazon Elastic Kubernetes Service (Amazon EKS) to run a container application. The EKS cluster stores sensitive information in the Kubernetes secrets object. The company wants to ensure that the information is encrypted. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use the container application to encrypt the information by using AWS Key Management Service (AWS KMS).
B.Enable secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS).
C.Implement an AWS Lambda function to encrypt the information by using AWS Key Management Service (AWS KMS).
D.Use AWS Systems Manager Parameter Store to encrypt the information by using AWS Key Management Service (AWS KMS).

Answer: B

Explanation:

- EKS integrates with KMS for secrets encryption directly.

- Option A manual encryption adds app overhead.

- Option C Lambda for encryption unnecessary.

- Option D Parameter Store is alternative but requires refactoring.

Question 214:
A company is designing a new multi-tier web application that consists of the following components:
• Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
• An Amazon RDS DB instance for data storage
A solutions architect needs to limit access to the application servers so that only the web servers can access them. Which solution will meet these requirements?

Options:
A.Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
B.Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
C.Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
D.Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.

Answer: D

Explanation:

- ALB provides Layer 7 routing and security group restrictions for controlled access.

- Option A PrivateLink not for same-VPC internal traffic.

- Option B VPC endpoint not designed for this case.

- Option C NLB works at L4 but doesn't enforce app-level security.

Question 215:
A company runs a critical, customer-facing application on Amazon Elastic Kubernetes Service (Amazon EKS). The application has a microservices architecture. The company needs to implement a solution that collects, aggregates, and summarizes metrics and logs from the application in a centralized location. Which solution meets these requirements?

Options:
A.Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.
B.Run AWS App Mesh in the existing EKS cluster. View the metrics and logs in the App Mesh console.
C.Configure AWS CloudTrail to capture data events. Query CloudTrail by using Amazon OpenSearch Service.
D.Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.

Answer: D

Explanation:

- CloudWatch Container Insights integrates directly with EKS for logs and metrics.

- Option A basic agent doesn't summarize container metrics well.

- Option B App Mesh is for service mesh, not logging.

- Option C CloudTrail tracks API calls, not metrics/logs.

Question 216:
A company has deployed its newest product on AWS. The product runs in an Auto Scaling group behind a Network Load Balancer. The company stores the product's objects in an Amazon S3 bucket. The company recently experienced malicious attacks against its systems. The company needs a solution that continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket. The solution must also report suspicious activity and display the information on a dashboard. Which solution will meet these requirements?

Options:
A.Configure Amazon Macie to monitor and report findings to AWS Config.
B.Configure Amazon Inspector to monitor and report findings to AWS CloudTrail.
C.Configure Amazon GuardDuty to monitor and report findings to AWS Security Hub.
D.Configure AWS Config to monitor and report findings to Amazon EventBridge.

Answer: C

Explanation:

- GuardDuty monitors malicious activity and integrates with Security Hub for dashboards.

- Option A Macie focuses on sensitive data, not threats.

- Option B Inspector is vulnerability scanning, not threat detection.

- Option D Config monitors compliance, not malicious activity.

Question 217:
A company wants to migrate an on-premises data center to AWS. The data center hosts a storage server that stores data in an NFS-based file system. The storage server holds 200 GB of data. The company needs to migrate the data without interruption to existing services. Multiple resources in AWS must be able to access the data by using the NFS protocol. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

Options:
A.Create an Amazon FSx for Lustre file system.
B.Create an Amazon Elastic File System (Amazon EFS) file system.
C.Create an Amazon S3 bucket to receive the data.
D.Manually use an operating system copy command to push the data into the AWS destination.
E.Install an AWS DataSync agent in the on-premises data center. Use a DataSync task between the on-premises location and AWS.

Answer: B, E

Explanation:

- EFS supports NFS and DataSync efficiently migrates from on-prem.

- Option A Lustre designed for HPC workloads, unnecessary.

- Option C S3 not NFS-compatible.

- Option D manual copy less efficient.

Question 218:
A company wants to use Amazon FSx for Windows File Server for its Amazon EC2 instances that have an SMB file share mounted as a volume in the us-east-1 Region. The company has a recovery point objective (RPO) of 5 minutes for planned system maintenance or unplanned service disruptions. The company needs to replicate the file system to the us-west-2 Region. The replicated data must not be deleted by any user for 5 years. Which solution will meet these requirements?

Options:
A.Create FSx in us-east-1 Single-AZ 2. Use AWS Backup daily backup plan with copy to us-west-2. Configure Vault Lock compliance mode for 5 years.
B.Create FSx in us-east-1 Multi-AZ. Use AWS Backup daily backup plan with copy to us-west-2. Configure Vault Lock governance mode for 5 years.
C.Create FSx in us-east-1 Multi-AZ. Use AWS Backup daily backup plan with copy to us-west-2. Configure Vault Lock compliance mode for 5 years.
D.Create FSx in us-east-1 Single-AZ 2. Use AWS Backup daily backup plan with copy to us-west-2. Configure Vault Lock governance mode for 5 years.

Answer: C

Explanation:

- Multi-AZ ensures HA, Backup Vault Lock compliance mode guarantees immutability.

- Option A Single-AZ less resilient.

- Option B governance mode less strict than compliance.

- Option D same as A with governance, not compliant.

Question 219:
A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified. Which action meets these requirements?

Options:
A.Create an IAM policy that prohibits changes to CloudTrail and attach it to the root user.
B.Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
C.Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
D.Create a service-linked role for CloudTrail with a policy condition that allows changes only from an ARN in the management account.

Answer: C

Explanation:

- SCPs prevent modification of CloudTrail across all member accounts.

- Option A cannot attach IAM policies to root users.

- Option B developers could still modify trails.

- Option D service-linked role not applicable.

Question 220:
A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance. Which type of storage should a solutions architect recommend to meet these requirements?

Options:
A.Instance store volume
B.Amazon ElastiCache for Memcached cluster
C.Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume
D.Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Answer: C

Explanation:

- Provisioned IOPS SSD EBS volumes deliver consistent, low-latency performance for critical workloads.

- Option A instance store is ephemeral, data lost when instance stops.

- Option B ElastiCache is in-memory cache, not durable storage.

- Option D Throughput HDD good for streaming, not low-latency.

Question 221:
An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region. Which solution will meet this requirement with the LEAST operational effort?

Options:
A.Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.
B.Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
C.Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.
D.Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Answer: A

Explanation:

- Cross-Region Replication automatically copies new objects with minimal setup.

- Option B CORS only controls access, not replication.

- Option C Lifecycle rules move within same bucket, not cross-Region.

- Option D Lambda adds unnecessary overhead.

Question 222:
A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's data architects have requested the ability to rapidly evolve their schema. Which solutions will meet these requirements and provide the MOST scalability? (Choose two.)

Options:
A.Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.
B.Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.
C.Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.
D.Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.
E.Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Answer: C, D

Explanation:

- DynamoDB with auto scaling handles large, spiky workloads.

- CloudFront + S3 serves static content globally with low latency.

- Option A DynamoDB on-demand is valid but costlier at this scale.

- Option B Aurora Serverless not best for unpredictable spikes at millions of users.

- Option E EC2 fleet for static content is overkill.

Question 223:
A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks. What is the MOST operationally efficient solution that meets these requirements?

Options:
A.Configure AWS Shield.
B.Configure AWS WAF.
C.Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.
D.Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Answer: B

Explanation:

- AWS WAF provides web application protection including SQLi and XSS filtering.

- Option A Shield protects against DDoS, not SQLi/XSS.

- Option C adds Shield, still doesn't handle app-level threats.

- Option D WAF on CloudFront adds complexity, direct WAF is enough.

Question 224:
A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network. However, the company does not want users to have to maintain another identity to access the resources. A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources. What should the solutions architect do to meet these requirements?

Options:
A.Create an IAM user for each user in the company. Attach the appropriate policies to each user.
B.Use Amazon Cognito with an Active Directory user pool. Create roles with the appropriate policies attached.
C.Define cross-account roles with the appropriate policies attached. Map the roles to the Active Directory groups.
D.Configure Security Assertion Markup Language (SAML) 2.0-based federation. Create roles with the appropriate policies attached. Map the roles to the Active Directory groups.

Answer: D

Explanation:

- SAML federation allows AD users to access AWS without separate identities.

- Option A IAM users scale poorly for 1500 users.

- Option B Cognito is for web/app authentication, not enterprise AD integration.

- Option C cross-account roles doesn't solve federation from AD.

Question 225:
A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights. Which configuration should the solutions architect choose to meet these requirements?

Options:
A.Configure Amazon CloudFront with AWS WAF.
B.Configure Application Load Balancers with AWS WAF.
C.Configure Amazon Route 53 with a geolocation policy.
D.Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

Explanation:

- Route 53 geolocation policy routes users by country/region for content rights.

- Option A CloudFront + WAF protects but doesn't control by geography.

- Option B ALB + WAF same issue.

- Option D geoproximity adjusts routing by bias, not strict geography.

Question 226:
A company stores its data on premises. The amount of data is growing beyond the company's available capacity. The company wants to migrate its data from the on-premises location to an Amazon S3 bucket. The company needs a solution that will automatically validate the integrity of the data after the transfer. Which solution will meet these requirements?

Options:
A.Order an AWS Snowball Edge device. Configure the Snowball Edge device to perform the online data transfer to an S3 bucket.
B.Deploy an AWS DataSync agent on premises. Configure the DataSync agent to perform the online data transfer to an S3 bucket.
C.Create an Amazon S3 File Gateway on premises. Configure the S3 File Gateway to perform the online data transfer to an S3 bucket.
D.Configure an accelerator in Amazon S3 Transfer Acceleration on premises. Configure the accelerator to perform the online data transfer to an S3 bucket.

Answer: B

Explanation:

- DataSync validates and verifies checksums during transfers.

- Option A Snowball works but better for PB-scale.

- Option C S3 File Gateway caches, not migration.

- Option D Transfer Acceleration speeds uploads but no validation.

Question 227:
A company wants to migrate two DNS servers to AWS. The servers host a total of approximately 200 zones and receive 1 million requests each day on average. The company wants to maximize availability while minimizing the operational overhead that is related to the management of the two servers. What should a solutions architect recommend to meet these requirements?

Options:
A.Create 200 new hosted zones in the Amazon Route 53 console. Import zone files.
B.Launch a single large Amazon EC2 instance. Import zone files. Configure CloudWatch alarms and notifications for downtime.
C.Migrate the servers to AWS by using AWS Server Migration Service (AWS SMS). Configure CloudWatch alarms for downtime.
D.Launch an EC2 instance in an Auto Scaling group across two AZs. Import zone files. Configure scaling alarms.

Answer: A

Explanation:

- Route 53 is managed DNS with HA, minimal overhead.

- Option B EC2 adds management burden.

- Option C SMS doesn't suit DNS workloads.

- Option D scaling EC2 for DNS adds complexity.

Question 228:
A global company runs its applications in multiple AWS accounts in AWS Organizations. The company's applications use multipart uploads to upload data to multiple Amazon S3 buckets across AWS Regions. The company wants to report on incomplete multipart uploads for cost compliance purposes. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Configure AWS Config with a rule to report the incomplete multipart upload object count.
B.Create a service control policy (SCP) to report the incomplete multipart upload object count.
C.Configure S3 Storage Lens to report the incomplete multipart upload object count.
D.Create an S3 Multi-Region Access Point to report the incomplete multipart upload object count.

Answer: C

Explanation:

- S3 Storage Lens provides metrics, including incomplete multipart uploads.

- Option A Config rules don't track multipart status.

- Option B SCPs can't report usage.

- Option D Multi-Region Access Points manage access, not reporting.

Question 229:
A company runs a production database on Amazon RDS for MySQL. The company wants to upgrade the database version for security compliance reasons. Because the database contains critical data, the company wants a quick solution to upgrade and test functionality without losing any data. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an RDS manual snapshot. Upgrade to the new version of Amazon RDS for MySQL.
B.Use native backup and restore. Restore the data to the upgraded new version of Amazon RDS for MySQL.
C.Use AWS Database Migration Service (AWS DMS) to replicate the data to the upgraded new version of Amazon RDS for MySQL.
D.Use Amazon RDS Blue/Green Deployments to deploy and test production changes.

Answer: D

Explanation:

- Blue/Green Deployments allow quick upgrade testing with zero data loss.

- Option A manual snapshot needs restore and downtime.

- Option B backup/restore manual and lengthy.

- Option C DMS adds unnecessary replication overhead.

Question 230:
A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning. How should the solutions architect address this issue in the MOST cost-effective manner?

Options:
A.Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
B.Create an AWS Lambda function triggered by an Amazon EventBridge scheduled event.
C.Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge scheduled event.
D.Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge scheduled event.

Answer: C

Explanation:

- ECS Fargate handles containerized jobs with no server management.

- Option A Reserved EC2 wastes cost.

- Option B Lambda max duration 15 minutes, not enough.

- Option D ECS EC2 requires instance management.

Question 231:
A social media company wants to store its database of user profiles, relationships, and interactions in the AWS Cloud. The company needs an application to monitor any changes in the database. The application needs to analyze the relationships between the data entities and to provide recommendations to users. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use Amazon Neptune to store the information. Use Amazon Kinesis Data Streams to process changes.
B.Use Amazon Neptune to store the information. Use Neptune Streams to process changes.
C.Use Amazon QLDB to store the information. Use Amazon Kinesis Data Streams to process changes.
D.Use Amazon QLDB to store the information. Use Neptune Streams to process changes.

Answer: B

Explanation:

- Neptune is purpose-built graph DB. Neptune Streams natively process changes.

- Option A Kinesis adds unnecessary complexity.

- Option C QLDB is ledger database, not graph.

- Option D mixing QLDB and Neptune Streams is invalid.

Question 232:
A company is creating a new application that will store a large amount of data. The data will be analyzed hourly and will be modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The needed amount of storage space will continue to grow for the next 6 months. Which storage solution should a solutions architect recommend to meet these requirements?

Options:
A.Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access.
B.Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
C.Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
D.Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Answer: C

Explanation:

- EFS provides scalable, shared storage across AZs for Linux instances.

- Option A Glacier archival, not frequent access.

- Option B EBS cannot attach across multiple AZs.

- Option D EBS not shareable among multiple instances.

Question 233:
A company manages an application that stores data on an Amazon RDS for PostgreSQL Multi-AZ DB instance. Increases in traffic are causing performance problems. The company determines that database queries are the primary reason for the slow performance. What should a solutions architect do to improve the application's performance?

Options:
A.Serve read traffic from the Multi-AZ standby replica.
B.Configure the DB instance to use Transfer Acceleration.
C.Create a read replica from the source DB instance. Serve read traffic from the read replica.
D.Use Amazon Kinesis Data Firehose between the application and Amazon RDS to increase the concurrency of database requests.

Answer: C

Explanation:

- Read replicas scale read queries without impacting writes.

- Option A standby is for failover, not reads.

- Option B Transfer Acceleration irrelevant.

- Option D Firehose doesn't apply to RDS.

Question 234:
A company collects 10 GB of telemetry data daily from various machines. The company stores the data in an Amazon S3 bucket in a source data account. The company has hired several consulting agencies to use this data for analysis. Each agency needs read access to the data for its analysts. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency. Which solution will meet these requirements?

Options:
A.Configure S3 global tables to replicate data for each agency.
B.Make the S3 bucket public for a limited time. Inform only the agencies.
C.Configure cross-account access for the S3 bucket to the accounts that the agencies own.
D.Set up an IAM user for each analyst in the source data account. Grant each user access to the S3 bucket.

Answer: C

Explanation:

- Cross-account bucket access grants secure access at account level.

- Option A global tables are for DynamoDB, not S3.

- Option B public bucket violates security.

- Option D IAM user per analyst not scalable.

Question 235:
A company uses Amazon FSx for NetApp ONTAP in its primary AWS Region for CIFS and NFS file shares. Applications that run on Amazon EC2 instances access the file shares. The company needs a storage disaster recovery (DR) solution in a secondary Region. The data that is replicated in the secondary Region needs to be accessed by using the same protocols as the primary Region. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create a Lambda function to copy data to an S3 bucket. Replicate the S3 bucket to the secondary Region.
B.Create a backup of the FSx for ONTAP volumes by using AWS Backup. Copy to secondary Region. Create new FSx from backup.
C.Create an FSx for ONTAP instance in the secondary Region. Use NetApp SnapMirror to replicate data.
D.Create an Amazon EFS volume. Replicate the volume to the secondary Region.

Answer: C

Explanation:

- SnapMirror provides native ONTAP replication with minimal setup.

- Option A S3 bucket copy breaks protocol compatibility.

- Option B backups require restore, not real-time DR.

- Option D EFS is different service, not protocol-compatible.

Question 236:

A development team is creating an event-based application that uses AWS Lambda functions. Events will be generated when files are added to an Amazon S3 bucket. The development team currently has Amazon SNS configured as the event target from Amazon S3. What should a solutions architect do to process the events from Amazon S3 in a scalable way?

Options:

A.Create an SNS subscription that processes the event in Amazon ECS before Lambda.
B.Create an SNS subscription that processes the event in Amazon EKS before Lambda.
C.Create an SNS subscription that sends the event to Amazon SQS. Configure the SQS queue to trigger a Lambda function.
D.Create an SNS subscription that sends the event to AWS SMS. Configure the Lambda function to poll from the SMS event.

Answer: C

Explanation:

- S3 → SNS → SQS → Lambda ensures durability and scalable event processing.

- Option A ECS adds unnecessary complexity.

- Option B EKS same issue.

- Option D SMS unrelated service.

Question 237:

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests. Which combination of AWS services would meet these requirements? (Choose two.)

Options:

A.AWS Fargate
B.AWS Lambda
C.Amazon DynamoDB
D.Amazon EC2 Auto Scaling
E.MySQL-compatible Amazon Aurora

Answer: B, C

Explanation:

- Lambda scales on-demand for unpredictable workloads.

- DynamoDB provides low-latency key-value queries.

Question 238:

A company collects and shares research data with the company's employees all over the world. The company wants to collect and store the data in an Amazon S3 bucket and process the data in the AWS Cloud. The company will share the data with the company's employees. The company needs a secure solution in the AWS Cloud that minimizes operational overhead. Which solution will meet these requirements?

Options:

A.Use an AWS Lambda function to create an S3 presigned URL. Instruct employees to use the URL.

B.Create an IAM user for each employee. Create an IAM policy for each employee to allow S3 access. Instruct employees to use the AWS Management Console.

C.Create an S3 File Gateway. Create a share for uploading and a share for downloading. Allow employees to mount shares on their local computers to use S3 File Gateway.

D.Configure AWS Transfer Family SFTP endpoints. Select the custom identity provider options. Use AWS Secrets Manager to manage the user credentials. Instruct employees to use Transfer Family.

Answer: A

Explanation:

- Presigned URLs provide secure temporary access with minimal overhead.

- Option B IAM users for each employee are unscalable.

- Option C File Gateway is for on-premises apps.

- Option D Transfer Family adds unnecessary complexity.

Question 239:

A company is building a new furniture inventory application. The company has deployed the application on a fleet of Amazon EC2 instances across multiple Availability Zones. The EC2 instances run behind an Application Load Balancer (ALB) in their VPC. A solutions architect has observed that incoming traffic seems to favor one EC2 instance, resulting in latency for some requests. What should the solutions architect do to resolve this issue?

Options:

A.Disable session affinity (sticky sessions) on the ALB.

B.Replace the ALB with a Network Load Balancer.

C.Increase the number of EC2 instances in each Availability Zone.

D.Adjust the frequency of the health checks on the ALB's target group.

Answer: A

Explanation:

- Sticky sessions route traffic to the same instance causing imbalance. Disabling them restores round-robin.

- Option B NLB doesn't solve stickiness.

- Option C adds capacity but not fair distribution.

- Option D health checks don't fix imbalance.

Question 240:
A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service (AWS KMS) keys. A solutions architect needs to design a solution that will ensure the required permissions are set correctly. Which combination of actions accomplish this? (Choose two.)

Options:
A.Attach the kms:Decrypt permission to the Lambda function's resource policy.
B.Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
C.Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
D.Create a new IAM policy with the kms:Decrypt permission and attach the policy to the Lambda function.
E.Create a new IAM role with the kms:Decrypt permission and attach the execution role to the Lambda function.

Answer: B, E

Explanation:

- Lambda execution role needs kms:Decrypt permission, and KMS key policy must allow role access.

- Option A not valid, Lambda resource policy doesn't apply here.

- Option C resource policy not used with KMS.

- Option D attaching IAM policy directly to function not possible.

Question 241:
A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts. The team must run this query once a month and provide a detailed analysis of the bill. Which solution is the MOST scalable and cost-effective way to meet these requirements?

Options:
A.Enable Cost and Usage Reports in the management account. Deliver reports to Amazon Kinesis. Use Amazon EMR for analysis.
B.Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3. Use Amazon Athena for analysis.
C.Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon S3. Use Amazon Redshift for analysis.
D.Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon Kinesis. Use Amazon QuickSight for analysis.

Answer: B

Explanation:

- CUR in S3 + Athena is cost-effective and serverless.

- Option A EMR is overkill for monthly queries.

- Option C CUR should be enabled at management account, not each member.

- Option D Kinesis unnecessary for batch reports.

Question 242:
A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases. What should a solutions architect do to meet these requirements?

Options:
A.Attach a Network Load Balancer to the Auto Scaling group.
B.Attach an Application Load Balancer to the Auto Scaling group.
C.Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.
D.Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Answer: A

Explanation:

- NLB supports UDP and scales automatically with Auto Scaling group.

- Option B ALB doesn't support UDP.

- Option C weighted policy doesn't provide scaling.

- Option D NAT instance doesn't load balance.

Question 243:
A company runs several websites on AWS for its different brands. Each website generates tens of gigabytes of web traffic logs each day. A solutions architect needs to design a scalable solution to give the company's developers the ability to analyze traffic patterns across all the company's websites. This analysis by the developers will occur on demand once a week over the course of several months. The solution must support queries with standard SQL. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Store the logs in Amazon S3. Use Amazon Athena for analysis.
B.Store the logs in Amazon RDS. Use a database client for analysis.
C.Store the logs in Amazon OpenSearch Service. Use OpenSearch Service for analysis.
D.Store the logs in an Amazon EMR cluster. Use a supported open-source framework for SQL-based analysis.

Answer: A

Explanation:

- S3 + Athena supports SQL queries on demand with minimal cost.

- Option B RDS costly for large log volumes.

- Option C OpenSearch unnecessary for periodic analysis.

- Option D EMR expensive for weekly jobs.

Question 244:
An international company has a subdomain for each country that the company operates in. The subdomains are formatted as example.com, country1.example.com, and country2.example.com. The company's workloads are behind an Application Load Balancer. The company wants to encrypt the website data that is in transit. Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Use AWS Certificate Manager (ACM) console to request a public certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
B.Use AWS Certificate Manager (ACM) console to request a private certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
C.Use AWS Certificate Manager (ACM) console to request a public and private certificate for the apex top domain example.com.
D.Validate domain ownership by email address. Switch to DNS validation by adding the required DNS records.
E.Validate domain ownership for the domain by adding the required DNS records to the DNS provider.

Answer: A, E

Explanation:

- Public ACM certs + DNS validation work for apex and subdomains.

- Option B private certs not for public websites.

- Option C mixing public/private not needed.

- Option D email validation less scalable.

Question 245:
A company is required to use cryptographic keys in its on-premises key manager. The key manager is outside of the AWS Cloud because of regulatory and compliance requirements. The company wants to manage encryption and decryption by using cryptographic keys that are retained outside of the AWS Cloud and that support a variety of external key managers from different vendors. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use AWS CloudHSM key store backed by a CloudHSM cluster.
B.Use an AWS Key Management Service (AWS KMS) external key store backed by an external key manager.
C.Use the default AWS KMS managed key store.
D.Use a custom key store backed by an AWS CloudHSM cluster.

Answer: B

Explanation:

- KMS external key store integrates with external key managers.

- Option A CloudHSM requires self-management.

- Option C default KMS stores keys in AWS, not allowed.

- Option D CloudHSM-based custom store high overhead.

Question 246:
A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing. Which solution will meet these requirements?

Options:
A.Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
B.Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
C.Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
D.Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances.

Answer: C

Explanation:

- FSx for Lustre provides sub-millisecond latency for HPC workloads and integrates with S3 for postprocessing.

- Option A EFS latency too high.

- Option B S3 not POSIX file system.

- Option D S3 sharing doesn't solve latency.

Question 247:
A gaming company is building an application with Voice over IP capabilities. The application will serve traffic to users across the world. The application needs to be highly available with an automated failover across AWS Regions. The company wants to minimize the latency of users without relying on IP address caching on user devices. What should a solutions architect do to meet these requirements?

Options:
A.Use AWS Global Accelerator with health checks.
B.Use Amazon Route 53 with a geolocation routing policy.
C.Create an Amazon CloudFront distribution that includes multiple origins.
D.Create an Application Load Balancer that uses path-based routing.

Answer: A

Explanation:

- Global Accelerator provides static IPs, global traffic routing, and automatic failover.

- Option B geolocation doesn't handle failover.

- Option C CloudFront caches HTTP, not real-time VoIP.

- Option D ALB is regional, not global.

Question 248:
A weather forecasting company needs to process hundreds of gigabytes of data with sub-millisecond latency. The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities. A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput. Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset. What should the solutions architect do to meet these requirements?

Options:
A.Use Amazon FSx for Lustre scratch file systems.
B.Use Amazon FSx for Lustre persistent file systems.
C.Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode.
D.Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.

Answer: B

Explanation:

- FSx Lustre persistent provides sustained high throughput with HA.

- Option A scratch not fault-tolerant.

- Option C/D EFS throughput lower than Lustre for HPC.

Question 249:
An ecommerce company runs a PostgreSQL database on premises. The database stores data by using high IOPS Amazon Elastic Block Store (Amazon EBS) block storage. The daily peak I/O transactions per second do not exceed 15,000 IOPS. The company wants to migrate the database to Amazon RDS for PostgreSQL and provision disk IOPS performance independent of disk storage capacity. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Configure the General Purpose SSD (gp2) EBS volume storage type and provision 15,000 IOPS.
B.Configure the Provisioned IOPS SSD (io1) EBS volume storage type and provision 15,000 IOPS.
C.Configure the General Purpose SSD (gp3) EBS volume storage type and provision 15,000 IOPS.
D.Configure the EBS magnetic volume type to achieve maximum IOPS.

Answer: C

Explanation:

- gp3 allows independent IOPS provisioning at lower cost.

- Option A gp2 cannot provision IOPS separately.

- Option B io1 works but is more expensive.

- Option D magnetic volumes don't support high IOPS.

Question 250:
A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Migrate to Amazon RDS for Microsoft SQL Server. Use read replicas for reporting purposes.
B.Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes.
C.Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes.
D.Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes.

Answer: A

Explanation:

- RDS SQL Server reduces management overhead and supports read replicas for analytics.

- Option B EC2 requires self-management.

- Option C DynamoDB incompatible with SQL Server workloads.

- Option D Aurora not compatible with SQL Server apps.

Question 251:
A company stores a large volume of image files in an Amazon S3 bucket. The images need to be readily available for the first 180 days. The images are infrequently accessed for the next 180 days. After 360 days, the images need to be archived but must be available instantly upon request. After 5 years, only auditors can access the images. The auditors must be able to retrieve the images within 12 hours. The images cannot be lost during this process.
A developer will use S3 Standard storage for the first 180 days. The developer needs to configure an S3 Lifecycle rule. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
B.Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
C.Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
D.Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

Answer: C

Explanation:

- Correct: Standard-IA after 180 days, Glacier Instant Retrieval at 360 days for instant access, Deep Archive after 5 years for compliance is the lowest-cost option.

- Option A is wrong because One Zone-IA reduces durability and is not suitable for compliance data.

- Option B is wrong because Glacier Flexible Retrieval does not guarantee instant retrieval.

- Option D is wrong because Flexible Retrieval also fails to meet "must be instantly available" requirement.

Question 252:

A company has a large data workload that runs for 6 hours each day. The company cannot lose any data while the process is running. A solutions architect is designing an Amazon EMR cluster configuration to support this critical data workload. Which solution will meet these requirements MOST cost-effectively?

Options:

A.Configure a long-running cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
B.Configure a transient cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
C.Configure a transient cluster that runs the primary node on an On-Demand Instance and the core nodes and task nodes on Spot Instances.
D.Configure a long-running cluster that runs the primary node on an On-Demand Instance, the core nodes on Spot Instances, and the task nodes on Spot Instances.

Answer: B

Explanation:

- Correct: Transient cluster with On-Demand master/core and Spot for tasks ensures no data loss and reduces cost for a daily 6-hour job.

- Option A is wrong because a long-running cluster would cost more when idle.

- Option C is wrong because Spot for core nodes risks data loss, unacceptable here.

- Option D is wrong because using Spot for core nodes in long-running setup is unreliable and expensive.

Question 253:

A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource. Which solution will meet these requirements?

Options:

A.Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.
B.Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.
C.Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.

D.Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Answer: B

Explanation:

- Correct: Lambda triggered by EventBridge with CloudTrail events ensures resources are auto-tagged with correct cost center.

- Option A is wrong because SCPs cannot dynamically enforce tag values from an external source.

- Option C is wrong because scheduled rules would miss real-time tagging.

- Option D is wrong because it only applies a default value, not user-specific cost centers.

Question 254:
A company recently migrated its web application to the AWS Cloud. The company uses an Amazon EC2 instance to run multiple processes to host the application. The processes include an Apache web server that serves static content. The Apache web server makes requests to a PHP application that uses a local Redis server for user sessions.
The company wants to redesign the architecture to be highly available and to use AWS managed solutions. Which solution will meet these requirements?

Options:
A.Use AWS Elastic Beanstalk to host the static content and the PHP application. Configure Elastic Beanstalk to deploy its EC2 instance into a public subnet. Assign a public IP address.
B.Use AWS Lambda to host the static content and the PHP application. Use an Amazon API Gateway REST API to proxy requests to the Lambda function. Set the API Gateway CORS configuration to respond to the domain name. Configure Amazon ElastiCache for Redis to handle session information.
C.Keep the backend code on the EC2 instance. Create an Amazon ElastiCache for Redis cluster that has Multi-AZ enabled. Configure the ElastiCache for Redis cluster in cluster mode. Copy the frontend resources to Amazon S3. Configure the backend code to reference the EC2 instance.
D.Configure an Amazon CloudFront distribution with an Amazon S3 endpoint to an S3 bucket that is configured to host the static content. Configure an Application Load Balancer that targets an Amazon Elastic Container Service (Amazon ECS) service that runs AWS Fargate tasks for the PHP application. Configure the PHP application to use an Amazon ElastiCache for Redis cluster that runs in multiple Availability Zones.

Answer: D

Explanation:

- Correct: CloudFront + S3 for static files, ECS Fargate for PHP backend, and Multi-AZ Redis cluster provide a scalable, HA managed solution.

- Option A is wrong because a single Elastic Beanstalk EC2 instance is not HA.

- Option B is wrong because PHP is not well-suited to Lambda execution model.

- Option C is wrong because it keeps reliance on EC2 and lacks scalability.

Question 255:
A company runs a web application on Amazon EC2 instances in an Auto Scaling group that has a target group. The company designed the application to work with session affinity (sticky sessions) for a better user experience.
The application must be available publicly over the internet as an endpoint. A WAF must be applied to the endpoint for additional security. Session affinity (sticky sessions) must be configured on the endpoint.
Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Create a public Network Load Balancer. Specify the application target group.
B.Create a Gateway Load Balancer. Specify the application target group.
C.Create a public Application Load Balancer. Specify the application target group.
D.Create a second target group. Add Elastic IP addresses to the EC2 instances.
E.Create a web ACL in AWS WAF. Associate the web ACL with the endpoint.

Answer: CE

Explanation:

- Correct: Application Load Balancer supports sticky sessions, and associating AWS WAF ACL secures the endpoint.

- Option A is wrong because NLB doesn't natively support sticky sessions.

- Option B is wrong because Gateway LB is for appliance-style deployments, not app affinity.

- Option D is wrong because Elastic IPs don't provide load balancing or stickiness.

Question 256:
A company runs a website that stores images of historical events. Website users need the ability to search and view images based on the year that the event in the image occurred. On average, users request each image only once or twice a year. The company wants a highly available solution to store and deliver the images to users. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Store images in Amazon Elastic Block Store (Amazon EBS). Use a web server that runs on Amazon EC2.
B.Store images in Amazon Elastic File System (Amazon EFS). Use a web server that runs on Amazon EC2.
C.Store images in Amazon S3 Standard. Use S3 Standard to directly deliver images by using a static website.
D.Store images in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Use S3 Standard-IA to directly deliver images by using a static website.

Answer: D

Explanation:

- Correct: S3 Standard-IA is cost-effective for rarely accessed data, still providing high availability.

- Option A is wrong because EBS tied to EC2 adds unnecessary cost and complexity.

- Option B is wrong because EFS is designed for shared file storage, not object delivery.

- ~~Option C is wrong because S3 Standard is more expensive for infrequently accessed images.~~

Question 257:
A company has multiple AWS accounts in an organization in AWS Organizations that different business units use. The company has multiple offices around the world. The company needs to update security group rules to allow new office CIDR ranges or to remove old CIDR ranges across the organization. The company wants to centralize the management of security group rules to minimize the administrative overhead that updating CIDR ranges requires. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create VPC security groups in the organization's management account. Update the security groups when a CIDR range update is necessary.
B.Create a VPC customer managed prefix list that contains the list of CIDRs. Use AWS Resource Access Manager (AWS RAM) to share the prefix list across the organization. Use the prefix list in the security groups across the organization.
C.Create an AWS managed prefix list. Use an AWS Security Hub policy to enforce the security group update across the organization. Use an AWS Lambda function to update the prefix list automatically when the CIDR ranges change.
D.Create security groups in a central administrative AWS account. Create an AWS Firewall Manager common security group policy for the whole organization. Select the previously created security groups as primary groups in the policy.

Answer: B

Explanation:

- Correct: Customer managed prefix list shared with RAM allows centralized CIDR management across accounts.

- Option A is wrong because manual updates in each account increase admin overhead.

- Option C is wrong because AWS does not provide managed prefix lists, only customer-managed.

- Option D is wrong because Firewall Manager is more complex and costlier than prefix lists for this use case.

Question 258:
A company uses an on-premises network-attached storage (NAS) system to provide file shares to its high performance computing (HPC) workloads. The company wants to migrate its latency-sensitive HPC workloads and its storage to the AWS Cloud. The company must be able to provide NFS and SMB multi-protocol access from the file system. Which solution will meet these requirements with the LEAST latency? (Choose two.)

Options:
A.Deploy compute optimized EC2 instances into a cluster placement group.
B.Deploy compute optimized EC2 instances into a partition placement group.
C.Attach the EC2 instances to an Amazon FSx for Lustre file system.
D.Attach the EC2 instances to an Amazon FSx for OpenZFS file system.
E.Attach the EC2 instances to an Amazon FSx for NetApp ONTAP file system.

Answer: AE

Explanation:

- Correct: FSx for NetApp ONTAP supports NFS and SMB protocols, and cluster placement groups ensure low latency for HPC.

- Option B is wrong because partition placement is for large distributed workloads, not low latency.

- Option C is wrong because FSx for Lustre is optimized for S3 integration, not SMB/NFS multi-protocol.

- Option D is wrong because FSx for OpenZFS supports NFS but not SMB multi-protocol.

Question 259:

A company is relocating its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized. Which AWS service should a solutions architect use to meet these requirements?

Options:
A.AWS DataSync with a VPC endpoint
B.AWS Direct Connect
C.AWS Snowball Edge Storage Optimized
D.AWS Storage Gateway

Answer: C

Explanation:

- Correct: Snowball Edge Storage Optimized is ideal for large one-time transfers of tens of TBs.

- Option A is wrong because DataSync requires network bandwidth, which is limited.

- Option B is wrong because setting up Direct Connect takes longer than 2 weeks.

- Option D is wrong because Storage Gateway is for hybrid storage, not bulk migration.

Question 260:

A company hosts an application on Amazon EC2 On-Demand Instances in an Auto Scaling group. Application peak hours occur at the same time each day. Application users report slow application performance at the start of peak hours. The application performs normally 2-3 hours after peak hours begin. The company wants to ensure that the application works properly at the start of peak hours. Which solution will meet these requirements?

Options:
A.Configure an Application Load Balancer to distribute traffic properly to the instances.
B.Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on memory utilization.
C.Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on CPU utilization.
D.Configure a scheduled scaling policy for the Auto Scaling group to launch new instances before peak hours.

Answer: D

Explanation:

- Correct: Scheduled scaling ensures EC2 instances are provisioned before peak hours begin, solving the performance issue.

- Option A is wrong because load balancing does not fix under-provisioning.

- Option B is wrong because memory-based scaling might not trigger in time.

- Option C is wrong because CPU scaling reacts after load increases, still causing delays.

Question 261:
A company runs applications on AWS that connect to the company's Amazon RDS database. The applications scale on weekends and at peak times of the year. The company wants to scale the database more effectively for its applications that connect to the database. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use Amazon DynamoDB with connection pooling with a target group configuration for the database. Change the applications to use the DynamoDB endpoint.
B.Use Amazon RDS Proxy with a target group for the database. Change the applications to use the RDS Proxy endpoint.
C.Use a custom proxy that runs on Amazon EC2 as an intermediary to the database. Change the applications to use the custom proxy endpoint.
D.Use an AWS Lambda function to provide connection pooling with a target group configuration for the database. Change the applications to use the Lambda function.

Answer: B

Explanation:

- Correct: RDS Proxy manages connections efficiently and reduces operational overhead compared to custom solutions.

- Option A is wrong because DynamoDB is not relational and requires re-engineering.

- Option C is wrong because custom proxies add management overhead.

- Option D is wrong because Lambda is not suited to manage persistent DB connection pools.

Question 262:
A company uses AWS Cost Explorer to monitor its AWS costs. The company notices that Amazon Elastic Block Store (Amazon EBS) storage and snapshot costs increase every month. However, the company does not purchase additional EBS storage every month. The company wants to optimize monthly costs for its current storage usage. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use logs in Amazon CloudWatch Logs to monitor the storage utilization of Amazon EBS. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.
B.Use a custom script to monitor space usage. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.
C.Delete all expired and unused snapshots to reduce snapshot costs.
D.Delete all nonessential snapshots. Use Amazon Data Lifecycle Manager to create and manage the snapshots according to the company's snapshot policy requirements.

Answer: D

Explanation:

- Correct: Data Lifecycle Manager automates snapshot management and deletion, reducing costs with minimal effort.

- Option A is wrong because Elastic Volumes resizing doesn't solve snapshot growth.

- Option B is wrong because scripting adds unnecessary operational overhead.

- Option C is wrong because it requires manual tracking and deletion.

Question 263:
A company is developing a new application on AWS. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster, an Amazon S3 bucket that contains assets for the application, and an Amazon RDS for MySQL database that contains the dataset for the application. The dataset contains sensitive information. The company wants to ensure that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket. Which solution will meet these requirements?

Options:
A.Create a new AWS Key Management Service (AWS KMS) customer managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the KMS key policy includes encrypt and decrypt permissions for the ECS task execution role.
B.Create an AWS Key Management Service (AWS KMS) AWS managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the S3 bucket policy specifies the ECS task execution role as a user.
C.Create an S3 bucket policy that restricts bucket access to the ECS task execution role. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in.
D.Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in. Create a VPC endpoint for Amazon S3. Update the S3 bucket policy to allow access from only the S3 VPC endpoint.

Answer: D

Explanation:

- Correct: Using VPC endpoints ensures private connectivity, and restricting S3 + RDS policies to ECS subnets ensures only ECS can access.

- Option A is wrong because encryption keys alone don't enforce access restriction.

- Option B is wrong because S3 bucket policy alone cannot restrict RDS access.

- Option C is wrong because it misses securing S3 access with VPC endpoint.

Question 264:
A company has a web application that runs on premises. The application experiences latency issues during peak hours. The latency issues occur twice each month. At the start of a latency issue, the application's CPU utilization immediately increases to 10 times its normal amount. The company wants to migrate the application to AWS to improve latency. The company also wants to scale the application automatically when application demand increases. The company will use AWS Elastic Beanstalk for application deployment. Which solution will meet these requirements?

Options:
A.Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale based on requests.
B.Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale based on requests.
C.Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale on a schedule.
D.Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale on predictive metrics.

Answer: D

Explanation:

- Correct: Burstable unlimited instances allow CPU spikes, and predictive scaling reduces latency during peak surges.

- Option A is wrong because scaling purely on requests may lag behind CPU spikes.

- Option B is wrong because compute-optimized instances alone don't prevent spikes.

- Option C is wrong because scheduled scaling won't help with unpredictable spikes.

Question 265:
A company has customers located across the world. The company wants to use automation to secure its systems and network infrastructure. The company's security team must be able to track and audit all incremental changes to the infrastructure. Which solution will meet these requirements?

Options:
A.Use AWS Organizations to set up the infrastructure. Use AWS Config to track changes.
B.Use AWS CloudFormation to set up the infrastructure. Use AWS Config to track changes.
C.Use AWS Organizations to set up the infrastructure. Use AWS Service Catalog to track changes.
D.Use AWS CloudFormation to set up the infrastructure. Use AWS Service Catalog to track changes.

Answer: B

Explanation:

- Correct: CloudFormation for infrastructure as code + AWS Config to continuously track changes satisfies auditing.

- Option A is wrong because Organizations alone doesn't provide change tracking.

- Option C is wrong because Service Catalog manages product deployment, not tracking.

- Option D is wrong because Service Catalog cannot track infrastructure drift.

Question 266:
A startup company is hosting a website for its customers on an Amazon EC2 instance. The website consists of a stateless Python application and a MySQL database. The website serves only a small amount of traffic. The company is concerned about the reliability of the instance and needs to migrate to a highly available architecture. The company cannot modify the application code. Which combination of actions should a solutions architect take to achieve high availability for the website? (Choose two.)

Options:
A.Provision an internet gateway in each Availability Zone in use.
B.Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance.
C.Migrate the database to Amazon DynamoDB, and enable DynamoDB auto scaling.
D.Use AWS DataSync to synchronize the database data across multiple EC2 instances.
E.Create an Application Load Balancer to distribute traffic to an Auto Scaling group of EC2 instances that are distributed across two Availability Zones.

Answer: BE

Explanation:

- Correct: RDS Multi-AZ ensures DB high availability, ALB + Auto Scaling ensures app tier HA.

- Option A is wrong because IGWs are per VPC, not per AZ.

- Option C is wrong because DynamoDB requires app code changes.

- Option D is wrong because DataSync is for migrations, not HA.

Question 267:
A company is moving its data and applications to AWS during a multiyear migration project. The company wants to securely access data on Amazon S3 from the company's AWS Region and from the company's on-premises location. The data must not traverse the internet. The company has established an AWS Direct Connect connection between its Region and its on-premises location. Which solution will meet these requirements?

Options:
A.Create gateway endpoints for Amazon S3. Use the gateway endpoints to securely access the data from the Region and the on-premises location.
B.Create a gateway in AWS Transit Gateway to access Amazon S3 securely from the Region and the on-premises location.
C.Create interface endpoints for Amazon S3. Use the interface endpoints to securely access the data from the Region and the on-premises location.
D.Use an AWS Key Management Service (AWS KMS) key to access the data securely from the Region and the on-premises location.

Answer: C

Explanation:

- Correct: S3 interface endpoints + Direct Connect ensure traffic stays private, not over internet.

- Option A is wrong because gateway endpoints work only within VPC, not on-premises.

- Option B is wrong because Transit Gateway doesn't provide direct S3 connectivity.

- Option D is wrong because KMS encryption doesn't enforce private networking.

Question 268:
A company created a new organization in AWS Organizations. The organization has multiple accounts for the company's development teams. The development team members use AWS IAM Identity Center (AWS Single Sign-On) to access the accounts. For each of the company's applications, the development teams must use a predefined application name to tag resources that are created. A solutions architect needs to design a solution that gives the development team the ability to create resources only if the application name tag has an approved value. Which solution will meet these requirements?

Options:
A.Create an IAM group that has a conditional Allow policy that requires the application name tag to be specified for resources to be created.
B.Create a cross-account role that has a Deny policy for any resource that has the application name tag.

C.Create a resource group in AWS Resource Groups to validate that the tags are applied to all resources in all accounts.
D.Create a tag policy in Organizations that has a list of allowed application names.

Answer: D

Explanation:

- Correct: Tag policies in AWS Organizations enforce allowed values across accounts automatically.

- Option A is wrong because IAM policies cannot enforce tag value lists.

- Option B is wrong because deny policies don't validate allowed tag values.

- Option C is wrong because Resource Groups only group resources, not enforce tag rules.

Question 269:
A company runs its databases on Amazon RDS for PostgreSQL. The company wants a secure solution to manage the master user password by rotating the password every 30 days. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use Amazon EventBridge to schedule a custom AWS Lambda function to rotate the password every 30 days.
B.Use the modify-db-instance command in the AWS CLI to change the password.
C.Integrate AWS Secrets Manager with Amazon RDS for PostgreSQL to automate password rotation.
D.Integrate AWS Systems Manager Parameter Store with Amazon RDS for PostgreSQL to automate password rotation.

Answer: C

Explanation:

- Correct: Secrets Manager integrates natively with RDS to automate rotation with no manual effort.

- Option A is wrong because Lambda adds operational maintenance.

- Option B is wrong because CLI-based manual rotation is not automated.

- Option D is wrong because Parameter Store does not support automatic DB rotation.

Question 270:
A company performs tests on an application that uses an Amazon DynamoDB table. The tests run for 4 hours once a week. The company knows how many read and write operations the application performs to the table each second during the tests. The company does not currently use DynamoDB for any other use case. A solutions architect needs to optimize the costs for the table. Which solution will meet these requirements?

Options:
A.Choose on-demand mode. Update the read and write capacity units appropriately.
B.Choose provisioned mode. Update the read and write capacity units appropriately.
C.Purchase DynamoDB reserved capacity for a 1-year term.
D.Purchase DynamoDB reserved capacity for a 3-year term.

Answer: B

Explanation:

- Correct: Provisioned mode is cheapest when predictable usage is known (4 hours/week with known RCU/WCU).

- Option A is wrong because on-demand is costlier for predictable workloads.

- Option C is wrong because reserved capacity is unnecessary for short, infrequent usage.

- Option D is wrong because 3-year reserved commitment is even less cost-effective.

Question 271:
A company runs its applications on Amazon EC2 instances. The company performs periodic financial assessments of its AWS costs. The company recently identified unusual spending. The company needs a solution to prevent unusual spending. The solution must monitor costs and notify responsible stakeholders in the event of unusual spending.
Which solution will meet these requirements?

Options:
A.Use an AWS Budgets template to create a zero spend budget.
B.Create an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost Management console.
C.Create AWS Pricing Calculator estimates for the current running workload pricing details.
D.Use Amazon CloudWatch to monitor costs and to identify unusual spending.

Answer: B

Explanation:

- Correct: Cost Anomaly Detection uses ML to detect unusual spending and can notify stakeholders.

- Option A is wrong because a zero spend budget is not practical and doesn't detect anomalies.

- Option C is wrong because Pricing Calculator only provides estimates, not monitoring.

- Option D is wrong because CloudWatch monitors performance metrics, not direct cost anomalies.

Question 272:
A marketing company receives a large amount of new clickstream data in Amazon S3 from a marketing campaign. The company needs to analyze the clickstream data in Amazon S3 quickly. Then the company needs to determine whether to process the data further in the data pipeline.

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

Options:
A.Create external tables in a Spark catalog. Configure jobs in AWS Glue to query the data.
B.Configure an AWS Glue crawler to crawl the data. Configure Amazon Athena to query the data.
C.Create external tables in a Hive metastore. Configure Spark jobs in Amazon EMR to query the data.
D.Configure an AWS Glue crawler to crawl the data. Configure Amazon Kinesis Data Analytics to use SQL to query the data.

Answer: B

Explanation:

- Correct: Glue crawler + Athena is serverless and low operational overhead for quick querying.

- Option A is wrong because Spark catalog setup requires more management.

- Option C is wrong because Hive + EMR cluster adds operational complexity.

- Option D is wrong because Kinesis Data Analytics is for streaming, not static S3 data.

Question 273:
A company runs an SMB file server in its data center. The file server stores large files that the company frequently accesses for up to 7 days after the file creation date. After 7 days, the company needs to be able to access the files with a maximum retrieval time of 24 hours. Which solution will meet these requirements?

Options:
A.Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
B.Create an Amazon S3 File Gateway to increase the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
C.Create an Amazon FSx File Gateway to increase the company's storage space. Create an Amazon S3 Lifecycle policy to transition the data after 7 days.
D.Configure access to Amazon S3 for each user. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Answer: B

Explanation:

- Correct: S3 File Gateway + Lifecycle to Glacier Deep Archive ensures cost-effective storage and 24-hour retrieval.

- Option A is wrong because DataSync alone doesn't provide lifecycle transitions.

- Option C is wrong because FSx File Gateway doesn't integrate directly with Glacier.

- Option D is wrong because Glacier Flexible Retrieval isn't as cost-efficient as Deep Archive.

Question 274:
A company runs a web application on Amazon EC2 instances in an Auto Scaling group. The application uses a database that runs on an Amazon RDS for PostgreSQL DB instance. The application performs slowly when traffic increases. The database experiences a heavy read load during periods of high traffic.
Which actions should a solutions architect take to resolve these performance issues? (Choose two.)

Options:
A.Turn on auto scaling for the DB instance.
B.Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.
C.Convert the DB instance to a Multi-AZ DB instance deployment. Configure the application to send read traffic to the standby DB instance.
D.Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.
E.Configure the Auto Scaling group subnets to ensure that the EC2 instances are provisioned in the same Availability Zone as the DB instance.

Answer: BD

Explanation:

- Correct: Read replica offloads read traffic, ElastiCache reduces DB queries for frequently accessed data.

- Option A is wrong because RDS scaling is vertical, not auto scaling.

- Option C is wrong because Multi-AZ provides HA, not read scaling.

- Option E is wrong because AZ colocation doesn't solve DB read load.

Question 275:
A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to run an application. The company creates one snapshot of each EBS volume every day to meet compliance requirements. The company wants to implement an architecture that prevents the accidental deletion of EBS volume snapshots. The solution must not change the administrative rights of the storage administrator user.
Which solution will meet these requirements with the LEAST administrative effort?

Options:
A.Create an IAM role that has permission to delete snapshots. Attach the role to a new EC2 instance. Use the AWS CLI from the new EC2 instance to delete snapshots.
B.Create an IAM policy that denies snapshot deletion. Attach the policy to the storage administrator user.
C.Add tags to the snapshots. Create retention rules in Recycle Bin for EBS snapshots that have the tags.
D.Lock the EBS snapshots to prevent deletion.

Answer: D

Explanation:

- Correct: Snapshot lock prevents deletion regardless of admin rights, minimal effort.

- Option A is wrong because it doesn't prevent deletion.

- Option B is wrong because it changes rights, against requirements.

- Option C is wrong because Recycle Bin is optional and relies on tags.

Question 276:
A company's application uses Network Load Balancers, Auto Scaling groups, Amazon EC2 instances, and databases that are deployed in an Amazon VPC. The company wants to capture information about traffic to and from the network interfaces in near real time in its Amazon VPC. The company wants to send the information to Amazon OpenSearch Service for analysis. Which solution will meet these requirements?

Options:
A.Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Streams to stream the logs from the log group to OpenSearch Service.
B.Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Firehose to stream the logs from the log group to OpenSearch Service.
C.Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Streams to stream the logs from the trail to OpenSearch Service.
D.Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Firehose to stream the logs from the trail to OpenSearch Service.

Answer: B

Explanation:

- Correct: Firehose integrates with CloudWatch Logs and delivers to OpenSearch with near real-time delivery.

- Option A is wrong because Data Streams requires custom consumers.

- Option C is wrong because CloudTrail is not for VPC Flow Logs.

- Option D is wrong because again CloudTrail is irrelevant for VPC network logs.

Question 277:
A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has managed node groups that are provisioned with On-Demand Instances.
The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create a managed node group that contains only Spot Instances.
B.Create two managed node groups. Provision one node group with On-Demand Instances. Provision the second node group with Spot Instances.
C.Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.
D.Create a managed node group that contains only On-Demand Instances.

Answer: A

Explanation:

- Correct: Spot Instances in managed node group reduce cost for infrequent dev workloads.

- Option B is wrong because On-Demand adds unnecessary cost.

- Option C is wrong because unmanaged Auto Scaling group increases overhead.

- Option D is wrong because On-Demand is expensive for infrequent testing.

Question 278:
A company stores sensitive data in Amazon S3. A solutions architect needs to create an encryption solution. The company needs to fully control the ability of users to create, rotate, and disable encryption keys with minimal effort for any data that must be encrypted. Which solution will meet these requirements?

Options:
A.Use default server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to store the sensitive data.
B.Create a customer managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).
C.Create an AWS managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).
D.Download S3 objects to an Amazon EC2 instance. Encrypt the objects by using customer managed keys. Upload the encrypted objects back into Amazon S3.

Answer: B

Explanation:

- Correct: Customer managed KMS key allows full control over key lifecycle (create, rotate, disable).

- Option A is wrong because SSE-S3 keys are fully managed by AWS.

- Option C is wrong because AWS managed KMS keys do not allow control.

- Option D is wrong because manual encryption adds unnecessary effort.

Question 279:
A company wants to back up its on-premises virtual machines (VMs) to AWS. The company's backup solution exports on-premises backups to an Amazon S3 bucket as objects. The S3 backups must be retained for 30 days and must be automatically deleted after 30 days. Which combination of steps will meet these requirements? (Choose three.)

Options:
A.Create an S3 bucket that has S3 Object Lock enabled.
B.Create an S3 bucket that has object versioning enabled.
C.Configure a default retention period of 30 days for the objects.
D.Configure an S3 Lifecycle policy to protect the objects for 30 days.
E.Configure an S3 Lifecycle policy to expire the objects after 30 days.
F.Configure the backup solution to tag the objects with a 30-day retention period.

Answer: ACE

Explanation:

- Correct: Object Lock + default 30-day retention + Lifecycle expiry ensures compliance retention and deletion.

- Option B is wrong because versioning isn't required.

- Option D is wrong because Lifecycle cannot enforce retention (only deletion).

- Option F is wrong because tagging doesn't enforce retention.

Question 280:
A solutions architect needs to copy files from an Amazon S3 bucket to an Amazon Elastic File System (Amazon EFS) file system and another S3 bucket. The files must be copied continuously. New files are added to the original S3 bucket consistently. The copied files should be overwritten only if the source file changes.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer only data that has changed.
B.Create an AWS Lambda function. Mount the file system to the function. Set up an S3 event notification to invoke the function when files are created and changed in Amazon S3. Configure the function to copy files to the file system and the destination S3 bucket.
C.Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer all data.
D.Launch an Amazon EC2 instance in the same VPC as the file system. Mount the file system. Create a script to routinely synchronize all objects that changed in the origin S3 bucket to the destination S3 bucket and the mounted file system.

Answer: A

Explanation:

- Correct: DataSync automates continuous incremental transfers with low effort.

- Option B is wrong because Lambda for large files adds complexity and scaling issues.

- Option C is wrong because transferring all data is inefficient.

- Option D is wrong because EC2 scripting adds high operational overhead.

Question 281:
A company uses Amazon EC2 instances and stores data on Amazon Elastic Block Store (Amazon EBS) volumes. The company must ensure that all data is encrypted at rest by using AWS Key Management Service (AWS KMS). The company must be able to control rotation of the encryption keys.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create a customer managed key. Use the key to encrypt the EBS volumes.
B.Use an AWS managed key to encrypt the EBS volumes. Use the key to configure automatic key rotation.
C.Create an external KMS key with imported key material. Use the key to encrypt the EBS volumes.
D.Use an AWS owned key to encrypt the EBS volumes.

Answer: A

Explanation:

- Correct: Customer managed key allows encryption and rotation control.

- Option B is wrong because AWS managed keys do not allow manual control.

- Option C is wrong because external KMS adds complexity.

- Option D is wrong because AWS owned keys offer no visibility or control.

Question 282:
A company needs a solution to enforce data encryption at rest on Amazon EC2 instances. The solution must automatically identify noncompliant resources and enforce compliance policies on findings.
Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A.Use an IAM policy that allows users to create only encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Config and AWS Systems Manager to automate the detection and remediation of unencrypted EBS volumes.
B.Use AWS Key Management Service (AWS KMS) to manage access to encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Lambda and Amazon EventBridge to automate the detection and remediation of unencrypted EBS volumes.
C.Use Amazon Macie to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.
D.Use Amazon Inspector to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.

Answer: A

Explanation:

- Correct: AWS Config rule + Systems Manager automates enforcement of encrypted volumes.

- Option B is wrong because KMS doesn't enforce encryption.

- Option C is wrong because Macie is for sensitive data discovery, not encryption enforcement.

- Option D is wrong because Inspector is for vulnerabilities, not encryption compliance.

Question 283:
A company is migrating its multi-tier on-premises application to AWS. The application consists of a single-node MySQL database and a multi-node web tier. The company must minimize changes to the application during the migration. The company wants to improve application resiliency after the migration.
Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.
B.Migrate the database to Amazon EC2 instances in an Auto Scaling group behind a Network Load Balancer.
C.Migrate the database to an Amazon RDS Multi-AZ deployment.
D.Migrate the web tier to an AWS Lambda function.
E.Migrate the database to an Amazon DynamoDB table.

Answer: AC

Explanation:

- Correct: ALB + Auto Scaling for web tier HA, and RDS Multi-AZ for DB resiliency.

- Option B is wrong because MySQL is not scalable across EC2 nodes easily.

- Option D is wrong because Lambda requires code refactor.

- Option E is wrong because DynamoDB is NoSQL and needs app redesign.

Question 284:
A company wants to migrate its web applications from on premises to AWS. The company is located close to the eu-central-1 Region. Because of regulations, the company cannot launch some of its applications in eu-central-1. The company wants to achieve single-digit millisecond latency.
Which solution will meet these requirements?

Options:
A.Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to an edge location in Amazon CloudFront.
B.Deploy the applications in AWS Local Zones by extending the company's VPC from eu-central-1 to the chosen Local Zone.
C.Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to the regional edge caches in Amazon CloudFront.
D.Deploy the applications in AWS Wavelength Zones by extending the company's VPC from eu-central-1 to the chosen Wavelength Zone.

Answer: B

Explanation:

- Correct: Local Zones bring AWS infrastructure closer to users with <10ms latency.

- Option A is wrong because CloudFront edge locations are for caching, not compute.

- Option C is wrong because regional caches don't run apps.

- Option D is wrong because Wavelength Zones are telecom-focused.

Question 285:
A company's ecommerce website has unpredictable traffic and uses AWS Lambda functions to directly access a private Amazon RDS for PostgreSQL DB instance. The company wants to maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections.
What should a solutions architect do to meet these requirements?

Options:
A.Point the client driver at an RDS custom endpoint. Deploy the Lambda functions inside a VPC.
B.Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions inside a VPC.
C.Point the client driver at an RDS custom endpoint. Deploy the Lambda functions outside a VPC.
D.Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions outside a VPC.

Answer: B

Explanation:

- Correct: RDS Proxy pools connections for Lambda to prevent overload.

- Option A is wrong because custom endpoint doesn't solve connection overload.

- Option C is wrong because outside VPC cannot access private DB.

- Option D is wrong because outside VPC also cannot reach private DB.

Question 286:
A company is creating an application. The company stores data from tests of the application in multiple on-premises locations.
The company needs to connect the on-premises locations to VPCs in an AWS Region in the AWS Cloud. The number of accounts and VPCs will increase during the next year. The network architecture must simplify the administration of new connections and must provide the ability to scale.
Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A.Create a peering connection between the VPCs. Create a VPN connection between the VPCs and the on-premises locations.
B.Launch an Amazon EC2 instance. On the instance, include VPN software that uses a VPN connection to connect all VPCs and on-premises locations.
C.Create a transit gateway. Create VPC attachments for the VPC connections. Create VPN attachments for the on-premises connections.
D.Create an AWS Direct Connect connection between the on-premises locations and a central VPC. Connect the central VPC to other VPCs by using peering connections.

Answer: C

Explanation:

- Correct: Transit Gateway centralizes and simplifies connections at scale.

- Option A is wrong because peering doesn't scale well.

- Option B is wrong because EC2 VPN software is high maintenance.

- Option D is wrong because peering from central VPC adds complexity.

Question 287:
A company that uses AWS needs a solution to predict the resources needed for manufacturing processes each month. The solution must use historical values that are currently stored in an Amazon S3 bucket. The company has no machine learning (ML) experience and wants to use a managed service for the training and predictions.
Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Deploy an Amazon SageMaker model. Create a SageMaker endpoint for inference.
B.Use Amazon SageMaker to train a model by using the historical data in the S3 bucket.
C.Configure an AWS Lambda function with a function URL that uses Amazon SageMaker endpoints to create predictions based on the inputs.
D.Configure an AWS Lambda function with a function URL that uses an Amazon Forecast predictor to create a prediction based on the inputs.
E.Train an Amazon Forecast predictor by using the historical data in the S3 bucket.

Answer: BD

Explanation:

- Correct: Forecast is managed ML for time-series prediction, trains directly on S3 data, and provides predictions.

- Option A is wrong because SageMaker requires ML expertise.

- Option C is wrong because SageMaker inference still requires trained models.

- Option E is wrong because Forecast training + Lambda predictor is already covered in B & D.

Question 288:
A company manages AWS accounts in AWS Organizations. AWS IAM Identity Center (AWS Single Sign-On) and AWS Control Tower are configured for the accounts. The company wants to manage multiple user permissions across all the accounts.
The permissions will be used by multiple IAM users and must be split between the developer and administrator teams. Each team requires different permissions. The company wants a solution that includes new users that are hired on both teams.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create individual users in IAM Identity Center for each account. Create separate developer and administrator groups in IAM Identity Center. Assign the users to the appropriate groups. Create a custom IAM policy for each group to set fine-grained permissions.
B.Create individual users in IAM Identity Center for each account. Create separate developer and administrator groups in IAM Identity Center. Assign the users to the appropriate groups. Attach AWS managed IAM policies to each user as needed for fine-grained permissions.
C.Create individual users in IAM Identity Center. Create new developer and administrator groups in IAM Identity Center. Create new permission sets that include the appropriate IAM policies for each group. Assign the new groups to the appropriate accounts. Assign the new permission sets to the new groups. When new users are hired, add them to the appropriate group.
D.Create individual users in IAM Identity Center. Create new permission sets that include the appropriate IAM policies for each user. Assign the users to the appropriate accounts. Grant additional IAM permissions to the users from within specific accounts. When new users are hired, add them to IAM Identity Center and assign them to the accounts.

Answer: C

Explanation:

- Correct: Permission sets + groups in IAM Identity Center scale easily across accounts.

- Option A is wrong because custom policies for each group increase management.

- Option B is wrong because attaching policies per user is inefficient.

- Option D is wrong because per-user permission sets add overhead.

Question 289:
A company wants to standardize its Amazon Elastic Block Store (Amazon EBS) volume encryption strategy. The company also wants to minimize the cost and configuration effort required to operate the volume encryption check.
Which solution will meet these requirements?

Options:
A.Write API calls to describe the EBS volumes and to confirm the EBS volumes are encrypted. Use Amazon EventBridge to schedule an AWS Lambda function to run the API calls.
B.Write API calls to describe the EBS volumes and to confirm the EBS volumes are encrypted. Run the API calls on an AWS Fargate task.
C.Create an AWS Identity and Access Management (IAM) policy that requires the use of tags on EBS volumes. Use AWS Cost Explorer to display resources that are not properly tagged. Encrypt the untagged resources manually.
D.Create an AWS Config rule for Amazon EBS to evaluate if a volume is encrypted and to flag the volume if it is not encrypted.

Answer: D

Explanation:

- Correct: AWS Config rule automates compliance checking with minimal cost.

- Option A is wrong because Lambda scripting adds management.

- Option B is wrong because Fargate is unnecessary overhead.

- Option C is wrong because tagging doesn't enforce encryption.

Question 290:
A company regularly uploads GB-sized files to Amazon S3. After the company uploads the files, the company uses a fleet of Amazon EC2 Spot Instances to transcode the file format. The company needs to scale throughput when the company uploads data from the on-premises data center to Amazon S3 and when the company downloads data from Amazon S3 to the EC2 instances.
Which solutions will meet these requirements? (Choose two.)

Options:
A.Use the S3 bucket access point instead of accessing the S3 bucket directly.
B.Upload the files into multiple S3 buckets.
C.Use S3 multipart uploads.
D.Fetch multiple byte-ranges of an object in parallel.
E.Add a random prefix to each object when uploading the files.

Answer: CD

Explanation:

- Correct: Multipart upload increases throughput for large files; parallel byte-range fetch optimizes download.

- Option A is wrong because access points are for access management, not performance.

- Option B is wrong because splitting buckets doesn't improve throughput.

- Option E is wrong because prefixes mainly help with key distribution, not needed in S3 today.

Question 291:
A solutions architect is designing a shared storage solution for a web application that is deployed across multiple Availability Zones. The web application runs on Amazon EC2 instances that are in an Auto Scaling group. The company plans to make frequent changes to the content. The solution must have strong consistency in returning the new content as soon as the changes occur.
Which solutions meet these requirements? (Choose two.)

Options:
A.Use AWS Storage Gateway Volume Gateway Internet Small Computer Systems Interface (iSCSI) block storage that is mounted to the individual EC2 instances.
B.Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on the individual EC2 instances.
C.Create a shared Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the individual EC2 instances.
D.Use AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group.
E.Create an Amazon S3 bucket to store the web content. Set the metadata for the Cache-Control header to nocache. Use Amazon CloudFront to deliver the content.

Answer: BE

Explanation:

- Correct: EFS is shared and strongly consistent, CloudFront + S3 with no-cache ensures fresh content delivery.

- Option A is wrong because Volume Gateway isn't designed for multi-AZ sharing.

- Option C is wrong because EBS cannot be mounted across AZs.

- Option D is wrong because DataSync isn't real-time for continuous changes.

Question 292:
A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these Regions.
Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

Options:
A.Create an A record with a latency policy.
B.Create an A record with a geolocation policy.
C.Create a CNAME record with a failover policy.
D.Create a CNAME record with a geoproximity policy.

Answer: B

Explanation:

- Correct: Geolocation routing directs traffic to the nearest region for performance.

- Option A is wrong because latency policy may not optimize globally.

- Option C is wrong because failover is for DR, not performance.

- Option D is wrong because geoproximity is complex and rarely used.

Question 293:
A company has a web application that includes an embedded NoSQL database. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone.
A recent increase in traffic requires the application to be highly available and for the database to be eventually consistent.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Replace the ALB with a Network Load Balancer. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
B.Replace the ALB with a Network Load Balancer. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).
C.Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
D.Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).

Answer: D

Explanation:

- Correct: DynamoDB is fully managed, HA, and eventually consistent, reducing ops overhead.

- Option A is wrong because NLB doesn't solve DB scaling.

- Option B is wrong because NLB is not needed for app-level HA.

- Option C is wrong because self-managed replication adds complexity.

Question 294:
A company is building a shopping application on AWS. The application offers a catalog that changes once each month and needs to scale with traffic volume. The company wants the lowest possible latency from the application. Data from each user's shopping cart needs to be highly available. User session data must be available even if the user is disconnected and reconnects.
What should a solutions architect do to ensure that the shopping cart data is preserved at all times?

Options:
A.Configure an Application Load Balancer to enable the sticky sessions feature (session affinity) for access to the catalog in Amazon Aurora.
B.Configure Amazon ElastiCache for Redis to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.
C.Configure Amazon OpenSearch Service to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.
D.Configure an Amazon EC2 instance with Amazon Elastic Block Store (Amazon EBS) storage for the catalog and shopping cart. Configure automated snapshots.

Answer: B

Explanation:

- Correct: ElastiCache provides low-latency in-memory storage for session/shopping cart data.

- Option A is wrong because Aurora is not designed for session data caching.

- Option C is wrong because OpenSearch is for search, not session caching.

- Option D is wrong because single EC2 + EBS isn't HA.

Question 295:
A company is building a microservices-based application that will be deployed on Amazon Elastic Kubernetes Service (Amazon EKS). The microservices will interact with each other. The company wants to ensure that the application is observable to identify performance issues in the future.
Which solution will meet these requirements?

Options:
A.Configure the application to use Amazon ElastiCache to reduce the number of requests that are sent to the microservices.
B.Configure Amazon CloudWatch Container Insights to collect metrics from the EKS clusters. Configure AWS X-Ray to trace the requests between the microservices.
C.Configure AWS CloudTrail to review the API calls. Build an Amazon QuickSight dashboard to observe the microservice interactions.
D.Use AWS Trusted Advisor to understand the performance of the application.

Answer: B

Explanation:

- Correct: CloudWatch Container Insights + X-Ray give observability into metrics and traces.

- Option A is wrong because caching does not provide observability.

- Option C is wrong because CloudTrail tracks API calls, not app interactions.

- Option D is wrong because Trusted Advisor checks best practices, not performance.

Question 296:
A company needs to provide customers with secure access to its data. The company processes customer data and stores the results in an Amazon S3 bucket.
All the data is subject to strong regulations and security requirements. The data must be encrypted at rest. Each customer must be able to access only their data from their AWS account. Company employees must not be able to access the data.
Which solution will meet these requirements?

Options:
A.Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the private certificate policy, deny access to the certificate for all principals except an IAM role that the customer provides.
B.Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In the S3 bucket policy, deny decryption of data for all principals except an IAM role that the customer provides.
C.Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In each KMS key policy, deny decryption of data for all principals except an IAM role that the customer provides.
D.Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the public certificate policy, deny access to the certificate for all principals except an IAM role that the customer provides.

Answer: C

Explanation:

- Correct: Separate KMS key per customer with restrictive key policies ensures secure per-customer access.

- Option A is wrong because ACM certificates are for TLS, not data encryption.

- Option B is wrong because bucket policy is insufficient to isolate keys.

- Option D is wrong because public cert policy isn't for encryption.

Question 297:
A solutions architect creates a VPC that includes two public subnets and two private subnets. A corporate security mandate requires the solutions architect to launch all Amazon EC2 instances in a private subnet. However, when the solutions architect launches an EC2 instance that runs a web server on ports 80 and 443 in a private subnet, no external internet traffic can connect to the server.
What should the solutions architect do to resolve this issue?

Options:
A.Attach the EC2 instance to an Auto Scaling group in a private subnet. Ensure that the DNS record for the website resolves to the Auto Scaling group identifier.
B.Provision an internet-facing Application Load Balancer (ALB) in a public subnet. Add the EC2 instance to the target group that is associated with the ALB. Ensure that the DNS record for the website resolves to the ALB.
C.Launch a NAT gateway in a private subnet. Update the route table for the private subnets to add a default route to the NAT gateway. Attach a public Elastic IP address to the NAT gateway.
D.Ensure that the security group that is attached to the EC2 instance allows HTTP traffic on port 80 and HTTPS traffic on port 443. Ensure that the DNS record for the website resolves to the public IP address of the EC2 instance.

Answer: B

Explanation:

- Correct: ALB in public subnet exposes the private instance securely.

- Option A is wrong because Auto Scaling group alone doesn't enable public access.

- Option C is wrong because NAT gateway is for outbound traffic, not inbound.

- Option D is wrong because private instances don't have public IPs.

Question 298:
A company is deploying a new application to Amazon Elastic Kubernetes Service (Amazon EKS) with an AWS Fargate cluster. The application needs a storage solution for data persistence. The solution must be highly available and fault tolerant. The solution also must be shared between multiple application containers.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create Amazon Elastic Block Store (Amazon EBS) volumes in the same Availability Zones where EKS worker nodes are placed. Register the volumes in a StorageClass object on an EKS cluster. Use EBS Multi-Attach to share the data between containers.
B.Create an Amazon Elastic File System (Amazon EFS) file system. Register the file system in a StorageClass object on an EKS cluster. Use the same file system for all containers.
C.Create an Amazon Elastic Block Store (Amazon EBS) volume. Register the volume in a StorageClass object on an EKS cluster. Use the same volume for all containers.
D.Create Amazon Elastic File System (Amazon EFS) file systems in the same Availability Zones where EKS worker nodes are placed. Register the file systems in a StorageClass object on an EKS cluster. Create an AWS Lambda function to synchronize the data between file systems.

Answer: B

Explanation:

- Correct: EFS is serverless, HA, fault tolerant, and shareable across containers.

- Option A is wrong because EBS volumes cannot span AZs.

- Option C is wrong because single EBS volume isn't HA.

- Option D is wrong because managing multiple EFS + Lambda sync is complex.

Question 299:
A company has an application that uses Docker containers in its local data center. The application runs on a container host that stores persistent data in a volume on the host. The container instances use the stored persistent data.
The company wants to move the application to a fully managed service because the company does not want to manage any servers or storage infrastructure.
Which solution will meet these requirements?

Options:
A.Use Amazon Elastic Kubernetes Service (Amazon EKS) with self-managed nodes. Create an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance. Use the EBS volume as a persistent volume mounted in the containers.
B.Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.
C.Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon S3 bucket. Map the S3 bucket as a persistent storage volume mounted in the containers.
D.Use Amazon Elastic Container Service (Amazon ECS) with an Amazon EC2 launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.

Answer: B

Explanation:

- Correct: ECS Fargate + EFS removes server/storage management with persistent shared storage.

- Option A is wrong because self-managed EKS adds infrastructure overhead.

- Option C is wrong because S3 is not a POSIX file system for containers.

- Option D is wrong because EC2 launch type requires server management.

Question 300:
A gaming company wants to launch a new internet-facing application in multiple AWS Regions. The application will use the TCP and UDP protocols for communication. The company needs to provide high availability and minimum latency for global users.
Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

Options:
A.Create internal Network Load Balancers in front of the application in each Region.
B.Create external Application Load Balancers in front of the application in each Region.
C.Create an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region.
D.Configure Amazon Route 53 to use a geolocation routing policy to distribute the traffic.
E.Configure Amazon CloudFront to handle the traffic and route requests to the application in each Region.

Answer: AC

Explanation:

- Correct: NLB supports TCP/UDP; Global Accelerator routes traffic to nearest region with low latency.

- Option B is wrong because ALB supports HTTP/HTTPS, not raw TCP/UDP.

- Option D is wrong because Route 53 geolocation isn't latency optimized.

- Option E is wrong because CloudFront is for HTTP/HTTPS caching, not TCP/UDP.

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

Options:
A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.
B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database on an EC2 instance. Enable EC2 Auto Recovery.
C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.
D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones. Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Answer: A

Explanation:

- A: Correct, Multi-AZ RDS avoids DB failure; ASG across AZs avoids app single point of failure.

- B: Single AZ = still single point of failure.

- C: Read replica doesn't automatically failover.

- D: EBS Multi-Attach isn't meant for production RDS-like workloads.

Question: 302
A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

Options:
A. Update the Kinesis Data Streams default settings by modifying the data retention period.
B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Answer: A

Explanation:

- A: Correct, default retention is 24h; app consumes every 2 days → data expired.

- B: KPL improves batching, but data loss cause is retention.

- C: Shards fix throughput, not data loss from retention.

- D: Versioning helps with overwrites, not missing data.

Question: 303

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3.

What should a solutions architect do to grant the permissions?

Options:

A. Add required IAM permissions in the resource policy of the Lambda function.

B. Create a signed request using the existing IAM credentials in the Lambda function.

C. Create a new IAM user and use the existing IAM credentials in the Lambda function.

D. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

Answer: D

Explanation:

- A: Lambda functions don't use resource policies for S3.

- B: Signed requests are insecure, not recommended.

- C: Storing IAM credentials inside Lambda is insecure.

- D: Correct, use execution role with least privilege.

Question: 304

A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

Options:

A. Set the Lambda function's runtime timeout value to 15 minutes.

B. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing.

C. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.

D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Answer: D

Explanation:

- A: Timeout won't fix dropped events.

- B: Replication doesn't solve event backlog.

- C: Still limited by concurrency/event loss.

- D: Correct, SQS acts as buffer and ensures reliability.

Question: 305

A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.
Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two.)

Options:
A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

Answer: D, E

Explanation:

- A: ALB scales automatically, no need.

- B: Internet gateway doesn't scale.

- C: Multi-Region not needed for demo.

- D: Correct, target tracking scales by CPU demand.

- E: Correct, scheduled scaling stops instances on weekends.

Question: 306

A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306.

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

Options:

A. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.

B. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.

C. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.

D. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.

E. Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.

Answer: C, D

Explanation:

- A: NACL unnecessary, SG sufficient.

- B: CIDR block approach is less secure than SG reference.

- C: Correct, SG for web tier allows HTTPS access.

- D: Correct, SG for DB allows access from web SG.

- E: Too restrictive, allow rules are enough.

Question: 308

A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored.

The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region.

Which solution will meet these requirements?

Options:

A. Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.

B. Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB. Process the data in Amazon ECS.

C. Use AWS Global Accelerator. Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

D. Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

Answer: B

Explanation:

- A: Route 53 adds DNS latency, not optimal.

- B: Correct, Global Accelerator + NLB supports UDP and fast failover.

- C: ALB does not support UDP.

- D: Same as C, ALB doesn't support UDP traffic.

Question: 309
A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances. Which replacement to the on-premises file share is MOST resilient and durable?

Options:
A. Migrate the file share to Amazon RDS.
B. Migrate the file share to AWS Storage Gateway.
C. Migrate the file share to Amazon FSx for Windows File Server.
D. Migrate the file share to Amazon Elastic File System (Amazon EFS).

Answer: C

Explanation:

- A: RDS is a database, not a file share.

- B: File gateway works, but not as resilient as FSx.

- C: Correct, FSx for Windows File Server fully supports SMB for IIS apps.

- D: EFS is NFS-based, not SMB.

Question: 310
A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.
Which solution will meet this requirement?

Options:
A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.
B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.
D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.

Answer: B

Explanation:

- A: Roles don't specify encryption settings.

- B: Correct, creating encrypted EBS volumes ensures data-at-rest encryption.

- C: Tags don't enforce encryption.

- D: Key policies don't automatically enforce encryption.

Question: 311
A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.
Which solution will meet these requirements?

Options:
A. Amazon DynamoDB
B. Amazon RDS for MySQL
C. MySQL-compatible Amazon Aurora Serverless
D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Answer: C

Explanation:

- A: DynamoDB would require major code changes.

- B: RDS for MySQL is managed, but doesn't auto-scale for unpredictable workloads.

- C: Correct, Aurora Serverless scales up/down based on demand.

- D: EC2-based MySQL adds operational overhead.

Question: 312

An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.

Which solution will meet these requirements?

Options:

A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.

B. Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.

C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.

D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.

Answer: D

Explanation:

- A: GuardDuty is for threat detection, not S3 block settings.

- B: Trusted Advisor is advisory, not preventative.

- C: RAM is not for S3; manual Lambda remediation adds overhead.

- D: Correct, account-level Block Public Access ensures all buckets stay private.

Question: 313

A company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

Options:

A. Create a separate application tier using EC2 instances dedicated to email processing.

B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).

C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).

D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Answer: B

Explanation:

- A: Adds complexity, not managed.

- B: Correct, SES is fully managed for email delivery.

- C: SNS is for pub/sub notifications, not email delivery at scale.

- D: Same as A, adds more overhead.

Question: 314
A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.
Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Answer: B

Explanation:

- A: Scheduled task = near real-time not guaranteed.

- B: Correct, File Gateway provides immediate S3 integration.

- C: Adds unnecessary coding overhead.

- D: Adds scripting and maintenance overhead.

Question: 315
A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.
Which solution will meet these requirements with the MOST operational efficiency?

Options:
A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: A

Explanation:

- A: Correct, Intelligent-Tiering auto-optimizes without admin work.

- B: Manual and labor-intensive.

- C: Glacier Instant Retrieval not optimal for all patterns.

- D: One Zone-IA risks durability, not cost-optimal for unknown patterns.

Question: 316
A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads.
Which combination of actions should a solutions architect take to resolve this issue? (Choose two.)

Options:
A. Configure an Amazon Redshift cluster.
B. Set up an Amazon CloudFront distribution.
C. Host the dynamic web content in Amazon S3.
D. Create a read replica for the RDS DB instance.
E. Configure a Multi-AZ deployment for the RDS DB instance.

Answer: BD

Explanation:

- A: Redshift is for analytics, not OLTP.

- B: Correct, CloudFront reduces latency for static content.

- C: Dynamic content can't be hosted in S3.

- D: Correct, read replica offloads read traffic.

- E: Multi-AZ improves HA, not performance.

Question: 317
A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.
The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.
Which solution will meet these requirements?

Options:
A. Purchase an EC2 Instance Savings Plan. Optimize the Lambda functions' duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
B. Purchase an EC2 Instance Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
C. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to the private subnet that contains the EC2 instances.
D. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.

Answer: C

Explanation:

- A: EC2 Instance Savings Plan only applies to EC2, not Lambda.

- B: Public subnet introduces latency and is unnecessary.

- C: Correct, Compute Savings Plan covers both EC2 + Lambda.

- D: Lambda service VPC won't reach EC2 in private subnets directly.

Question: 318
A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.
The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.
Which solution will meet these requirements while complying with the principle of least privilege?

Options:
A. Attach the Administrator Access policy to the development account users.
B. Add the development account as a principal in the trust policy of the role in the production account.
C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
D. Create a user in the production account with unique credentials for each team member.

Answer: B

Explanation:

- A: Overly permissive, violates least privilege.

- B: Correct, role trust policy allows cross-account access.

- C: Weakens security, unrelated.

- D: Creates unnecessary users, not efficient.

Question: 319
A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest.

An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any IAM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes.

Which combination of steps will meet these requirements? (Choose two.)

Options:
A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.
B. Create an IAM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
C. Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
D. Update the IAM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
E. In the Organizations management account, specify the Default EBS volume encryption setting.

Answer: CE

Explanation:

- A: Only sets account attribute, doesn't enforce across org.

- B: Permission boundaries not org-wide.

- C: Correct, SCP enforces encrypted volumes across OU.

- D: Updating IAM policies per account adds overhead.

- E: Correct, default EBS encryption ensures compliance.

Question: 320

A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible.

Which solution will meet these requirements?

Options:

A. Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.

B. Use an Amazon RDS Multi-AZ DB cluster deployment. Create two read replicas and point the read workload to the read replicas.

C. Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.

D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint.

Answer: D

Explanation:

- A: Legacy Multi-AZ instance deployments don't give reader endpoint.

- B: Extra replicas increase cost.

- C: In DB instance deployment, secondary is not for reads.

- D: Correct, Multi-AZ cluster supports reader endpoint + <40s failover.

Question: 321

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers.

The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions.

Which solution will meet these requirements?

Options:

A. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.

B. Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.

C. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

D. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

Answer: B

Explanation:

- A: EBS cannot be directly mounted to Transfer Family.

- B: Correct, EFS + Transfer Family supports high IOPS and fine-grained access.

- C: S3 is valid but not high IOPS for this use case.

- D: S3 internal only, doesn't satisfy IOPS requirement.

Question: 322
A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.
The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.
Which design should a solutions architect recommend to meet these requirements?

Options:
A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.
B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.
C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.
D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.

Answer: D

Explanation:

- A: Lambda not suitable for 1GB startup.

- B: ALB adds extra overhead; App Mesh unnecessary.

- C: Lambda limited by startup package size.

- D: Correct, ECS with SQS provides scalable container-based services.

Question: 323
A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{       "Statement": [
            {
                "Action": [
                    "ssm:ListDocuments",
                    "ssm:GetDocument"
                ],
                "Effect": "Allow",
                "Resource": "*",
                "Sid": ""
            }
        ],
        "Version": "2012-10-17"
}
```

Which IAM principals can the solutions architect attach this policy to? (Choose two.)

Options:
A. Role
B. Group
C. Organization
D. Amazon Elastic Container Service (Amazon ECS) resource
E. Amazon EC2 resource

Answer: AB

Explanation:

- A: Correct, roles can have policies attached.

- B: Correct, groups can have policies attached.

- C: SCPs apply to Organizations, not IAM identity policies.

- D: ECS resources don't accept identity policies.

- E: EC2 resources accept resource-based, not identity-based policies.

Question: 324
A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day.
The company needs to scale out and scale in more instances based on workload.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
B. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.
C. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
D. Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

Answer: B

Explanation:

- A: Fargate good but costlier.

- B: Correct, Reserved for always-on + Spot for variable = most cost effective.

- C: Wrong allocation.

- D: Spot for frontend risks availability.

Question: 325
A company uses high block storage capacity to run its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity.
Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?

Options:
A. GP2 volume type
B. io2 volume type
C. GP3 volume type
D. io1 volume type

Answer: C

Explanation:

- A: GP2 ties IOPS to size.

- B: io2 is high performance, expensive.

- C: Correct, GP3 allows provisioned IOPS independent of size.

- D: io1 similar to io2, costlier.

Question: 326
A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit access at all levels of the stored data. The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.
Which solution will meet these requirements?

Options:
A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Answer: A

Explanation:

- A: Correct, DataSync migrates + CloudTrail data events satisfy audit.

- B: Snowcone for edge/offline, not best for this.

- C: Transfer Acceleration unnecessary, doesn't address audit.

- D: Storage Gateway not suited for one-time migration.

Question: 327

A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.
What should the solutions architect do to meet these requirements?

Options:

A. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.
B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.
C. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.
D. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an Auto Scaling group.

Answer: B

Explanation:

- A: Lambda not for Tomcat.

- B: Correct, Elastic Beanstalk automates Tomcat + HA + DB.

- C: ElastiCache not a relational DB.

- D: Manual scaling, high overhead.

Question: 328
A serverless application uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB.
The Lambda function needs permissions to read and write to the DynamoDB table.
Which solution will give the Lambda function access to the DynamoDB table MOST securely?

Options:
A. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration.
B. Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.
C. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.
D. Create an IAM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.

Answer: B

Explanation:

- A: Storing keys in env variables insecure.

- B: Correct, IAM role with Lambda trust is best practice.

- C: Parameter Store adds unnecessary complexity.

- D: DynamoDB can't be a trusted principal.

Question: 329

The following IAM policy is attached to an IAM group. This is the only policy applied to the group. What are the effective IAM permissions of this policy for group members?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

Options:

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.

B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).

C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.

D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Answer: D

Explanation:

- A: Not true, MFA requirement exists.

- B: Deny is conditional, not global.

- C: Permissions restricted to us-east-1, not all Regions.

- D: Correct, applies only in us-east-1 with MFA.

Question: 330

A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports. The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

Options:

A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.

B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.

C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.

D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.

E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Answer: BC

Explanation:

- A: EC2 Spot adds management and cost.

- B: Correct, Lambda auto-triggers conversion.

- C: Correct, Glacier reduces storage cost for infrequent ML use.

- D: One Zone-IA is riskier, less durable.

- E: RRS is deprecated, not compliant.

Question: 331

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

What should a solutions architect do to meet these requirements?

Options:

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

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

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

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

Answer: B

Explanation:

- A: Memcached lacks persistence.

- B: Correct, Redis supports sorted sets + persistence.

- C: CloudFront caches static content, not dynamic scoreboard.

- D: RDS read replica adds latency, not real-time.

Question: 332

A company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards. Which solution will meet these requirements with the LEAST operational overhead?

Options:

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

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

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

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

Answer: B

Explanation:

- A: Glue ML transforms are limited.

- B: Correct, SageMaker for ML + QuickSight BI dashboards.

- C: Marketplace AMIs add manual overhead.

- D: QuickSight is BI only, not ML training.

Question: 333
A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.
Which solution will meet these requirements?

Options:
A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.
B. Create a custom trail in AWS CloudTrail to prevent tag modification.
C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.
D. Create custom Amazon CloudWatch logs to prevent tag modification.

Answer: C

Explanation:

- A: Config detects, doesn't prevent.

- B: CloudTrail records, doesn't block.

- C: Correct, SCP enforces organization-wide restrictions.

- D: CloudWatch logs cannot block actions.

Question: 334
A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.
What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

Options:
A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Answer: A

Explanation:

- A: Correct, pre-provision DR + DynamoDB global tables + DNS failover ensures minimal downtime.

- B: Cold standby, causes downtime.

- C: DynamoDB global correct but EC2 is cold standby.

- D: More complex than required.

Question: 335

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

Which solution will migrate the database MOST cost-effectively?

Options:

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

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

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

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

Answer: A

Explanation:

- A: Correct, Snowball Edge + DMS ongoing replication = efficient for 20TB.

- B: Snowmobile is for PB scale.

- C: Compute Optimized unnecessary.

- D: 1Gbps too slow for 20TB in 2 weeks.

Question: 336
A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased. The company wants to accommodate the larger workload without adding infrastructure.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.
B. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.
C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.
D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.

Answer: A

Explanation:

- A: Correct, Reserved reduces cost + scale up DB instance.

- B: Multi-AZ improves HA, not workload.

- C: Horizontal scaling not supported by RDS.

- D: On-demand more expensive.

Question: 337
A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.
What should a solutions architect recommend?

Options:
A. Deploy Amazon Inspector and associate it with the ALB.
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Answer: B

Explanation:

- A: Inspector is for vulnerabilities, not DDoS.

- B: Correct, AWS WAF with rate-limiting blocks illegitimate requests.

- C: NACLs not flexible for dynamic IPs.

- D: GuardDuty only detects threats.

Question: 338
A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.
What is the MOST secure way for the company to share the database with the auditor?

Options:
A. Create a read replica of the database. Configure IAM standard database authentication to grant the auditor access.
B. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.
C. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the S3 bucket.
D. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key.

Answer: D

Explanation:

- A: Requires DB-level access, less secure.

- B: Exporting data insecure.

- C: Keys sharing is insecure.

- D: Correct, encrypted snapshot sharing with KMS access is secure.

Question: 339
A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.
Which solution resolves this issue with the LEAST operational overhead?

Options:
A. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.
B. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC. Update the routes and create new resources in the subnets of the second VPC.
C. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPC. Update the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.
D. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.

Answer: A

Explanation:

- A: Correct, simplest way is to add additional CIDR to same VPC.

- B: VPC peering adds overhead.

- C: Transit Gateway overkill.

- D: VPN adds complexity.

Question: 340

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

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

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

Options:

A. Import the RDS snapshot directly into Aurora.
B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.
C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.
D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.
E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Answer: AC

Explanation:

- A: Correct, RDS snapshot can import directly to Aurora.

- B: Not required, snapshots don't import via S3.

- C: Correct, S3 + dump import into Aurora possible.

- D: DMS not needed for snapshot.

- E: Dump doesn't require DMS.

Question: 341

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

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

Options:

A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.
B. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.
C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.
D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Answer: C

Explanation:

- A: Reserved doesn't address static content load.

- B: Spot is risky for static content delivery.

- C: Correct, CloudFront + S3 offloads static content.

- D: Lambda/API Gateway not efficient for static hosting.

Question: 342
A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.
B. Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.
C. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.
D. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.

Answer: D

Explanation:

- A: Duplication increases storage.

- B: Per-account management overhead.

- C: Data Exchange for external, not internal org.

- D: Correct, Lake Formation tag-based access control best for cross-account.

Question: 343
A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.
What should a solutions architect do to accomplish this?

Options:
A. Use Amazon S3 with Transfer Acceleration to host the application.
B. Use Amazon S3 with CacheControl headers to host the application.
C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: A

Explanation:

- A: Correct, S3 Transfer Acceleration reduces latency for large uploads/downloads.

- B: CacheControl doesn't improve global upload performance.

- C: EC2 adds more cost/overhead.

- D: ElastiCache doesn't solve upload latency.

Question: 344

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone. An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

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

Options:

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

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

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

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

Answer: B

Explanation:

- A: Doesn't provide HA for EC2 layer.

- B: Correct, Multi-AZ DB + ALB + Auto Scaling across AZs ensures HA.

- C: Overengineered.

- D: Spot not ideal for reliability.

Question: 345

A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection. After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window. Which solution will meet these requirements?

Options:

A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task. Start the transfer to an Amazon S3 bucket.

B. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

C. Use rsync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.

D. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

Answer: A

Explanation:

- A: Correct, DataSync with Direct Connect enables ongoing sync + access.

- B: Snowball works offline, not continuous updates.

- C: rsync lacks efficiency for 700 TB.

- D: Tape backup not modern solution.

Question: 346
A company stores data in PDF format in an Amazon S3 bucket. The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Turn on the S3 Versioning feature for the S3 bucket. Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.
B. Turn on S3 Object Lock with governance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

Answer: D

Explanation:

- A: Versioning doesn't enforce retention.

- B: Governance mode allows overrides.

- C: Compliance mode correct, but manually recopying adds overhead.

- D: Correct, Compliance mode + Batch Ops automates compliance.

Question: 347
A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.
What should a solutions architect do to route traffic to multiple Regions?

Options:
A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.
B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.
C. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.
D. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

Answer: B

Explanation:

- A: Route 53 DNS failover only, not best for API Gateway.

- B: Correct, CloudFront multi-origin with health checks ensures global failover.

- C: Transit gateway is for VPC connectivity.

- D: ALB cannot target API Gateway endpoints.

Question: 348
A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.
What should a solutions architect do to mitigate any single point of failure in this architecture?

Options:
A. Add a set of VPNs between the Management and Production VPCs.
B. Add a second virtual private gateway and attach it to the Management VPC.
C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Answer: C

Explanation:

- A: Cross-VPC VPN not relevant.

- B: VGW redundancy alone not enough.

- C: Correct, second customer gateway ensures redundancy.

- D: Peering redundancy doesn't fix device SPOF.

Question: 349

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

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

Options:

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

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

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

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

Answer: B

Explanation:

- A: RDS for Oracle doesn't allow privileged features.

- B: Correct, RDS Custom supports custom configs and privileged access.

- C: EC2 adds more management overhead.

- D: PostgreSQL requires rewriting, not quick.

Question: 350

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

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

Options:

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

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

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

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

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

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

Answer: CEF

Explanation:

- A: Doesn't refactor properly.

- B: Single DB in one AZ not HA.

- C: Correct, multi-tier refactor.

- E: Correct, ELB for scalability.

- F: Correct, RDS Multi-AZ for HA.

Question: 351
A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS. Which activities will be managed by the company's operational team? (Choose three.)

Options:
A. Management of the Amazon RDS infrastructure layer, operating system, and platforms
B. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window
C. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection
D. Installation of patches for all minor and major database versions for Amazon RDS
E. Ensure the physical security of the Amazon RDS infrastructure in the data center
F. Encryption of the data that moves in transit through Direct Connect

Answer: BCF

Explanation:

- A: Managed by AWS, not customer.

- B: Correct, operational team configures DB instance and maintenance.

- C: Correct, ECS extra monitoring/patching is customer responsibility.

- D: Patching managed by AWS.

- E: Physical security is AWS responsibility.

- F: Correct, customer responsible for in-transit encryption.

Question: 352
A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The company wants to optimize the costs to run the job.
Which solution will meet these requirements?

Options:
A. Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.
B. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.
C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.
D. Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.

Answer: B

Explanation:

- A: Fargate works, but Lambda is simpler and cheaper.

- B: Correct, Lambda + EventBridge perfectly matches short scheduled jobs.

- C: Adds unnecessary overhead.

- D: Stopping/starting EC2 still incurs overhead.

Question: 353
A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.
Which solution will meet these requirements?

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

Answer: D

Explanation:

- A: Governance mode allows deletion by privileged users.

- B: Lifecycle manager lacks compliance lock.

- C: S3 File Gateway not for compliance backups.

- D: Correct, compliance mode prevents alteration/deletion.

Question: 354

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

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

Options:

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

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

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

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

Answer: C

Explanation:

- A: Systems Manager Inventory doesn't provide cross-account diagrams.

- B: Step Functions requires manual effort.

- C: Correct, Workload Discovery auto-generates diagrams.

- D: X-Ray only traces applications, not infra.

Question: 355

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

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

Options:

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

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

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

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

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

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

Answer: BDF

Explanation:

- A: Incorrect, Cost and Usage reports not used here.

- B: Correct, budgets via Billing dashboard.

- C: IAM user not needed.

- D: Correct, IAM role enables automation.

- E: Config rule irrelevant.

- F: Correct, SCP prevents further provisioning.

Question: 356

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

Which solution will meet these requirements MOST cost-effectively?

Options:

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

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

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

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

Answer: C

Explanation:

- A: Running DR resources increases cost.

- B: Snapshots possible, but manual overhead.

- C: Correct, AWS Backup with cross-Region automated backups is simplest.

- D: Running duplicate EC2s increases cost.

Question: 357

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

Which solution will meet these requirements?

Options:

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

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

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

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

Answer: C

Explanation:

- A: DataSync doesn't support AS2.

- B: AppFlow not for AS2.

- C: Correct, AWS Transfer Family supports AS2 + integrates with custom auth.

- D: Storage Gateway not relevant here.

Question: 358

A solutions architect is designing a REST API in Amazon API Gateway for a cash payback service. The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.
Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? (Choose two.)

Options:
A. Amazon EC2
B. AWS Lambda
C. Amazon RDS
D. Amazon DynamoDB
E. Amazon Elastic Kubernetes Service (Amazon EKS)

Answer: BC

Explanation:

- A: EC2 adds admin overhead.

- B: Correct, Lambda for compute.

- C: Correct, RDS for relational data.

- D: DynamoDB is NoSQL.

- E: EKS too complex.

Question: 359

A company uses AWS Organizations to run workloads within multiple AWS accounts. A tagging policy adds department tags to AWS resources when the company creates tags. An accounting team needs to determine spending on Amazon EC2 consumption. The accounting team must determine which departments are responsible for the costs regardless of AWS account. The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer.
Which solution meets these requirements in the MOST operationally efficient way?

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

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

Answer: A

Explanation:

- A: Correct, activate cost allocation tags in management account, then use Cost Explorer.

- B: AWS-defined tags don't include department.

- C & D: Done from member account, not centralized.

Question: 360
A company wants to securely exchange data between its software as a service (Saa) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account. Which solution will meet these requirements?

Options:
A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.
B. Create an AWS Step Functions workflow. Define the task to transfer the data securely from Salesforce to Amazon S3.
C. Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.
D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.

Answer: C

Explanation:

- A: Lambda possible but adds overhead.

- B: Step Functions is orchestration, not direct secure transfer.

- C: Correct, AppFlow securely transfers Salesforce data with KMS encryption.

- D: Custom connector adds unnecessary dev effort.

Question: 361
A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.
Which solution will meet these requirements?

Options:
A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.
B. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB.
C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.
D. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin.

Answer: B

Explanation:

- A: ALB doesn't support UDP.

- B: Correct, NLB with Global Accelerator supports TCP + UDP, lowest latency.

- C: CloudFront is for HTTP/HTTPS, not raw TCP/UDP.

- D: Same issue, ALB not suitable.

Question: 362
A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high the workload does not process orders fast enough.
What should a solutions architect do to write the orders reliably to the database as quickly as possible?

Options:
A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.
B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
C. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.
D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

Answer: B

Explanation:

- A: SNS is pub-sub, not guaranteed order persistence.

- B: Correct, SQS decouples traffic bursts and ensures durability.

- C: SNS not designed for durable queueing.

- D: Conditional queueing not optimal.

Question: 363
An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible. Data processing will require 1 GB of memory and will finish within 30 seconds.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use AWS Glue with a Scala job
B. Use Amazon EMR with an Apache Spark script
C. Use AWS Lambda with a Python script
D. Use AWS Glue with a PySpark job

Answer: C

Explanation:

- A: Glue is overkill and more expensive.

- B: EMR is not cost-efficient for 2 MB files.

- C: Correct, Lambda handles short bursts, memory, and time well.

- D: Glue PySpark is also unnecessary overhead.

Question: 364
A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.
Which solution meets these requirements?

Options:
A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Answer: A

Explanation:

- A: Correct, convert to Multi-AZ with minimal downtime, no code changes.

- B: Snapshot restore requires new endpoint, some code changes.

- C: Read replica not HA.

- D: EC2 for RDS not possible.

Question: 365
A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.
Which solution will meet these requirements?

Options:
A. Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
B. Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
D. Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

Answer: C

Explanation:

- A/D: gp2/gp3 not supported for Multi-Attach.

- B: st1 also not supported.

- C: Correct, io1/io2 volumes support Multi-Attach.

Question: 366
A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.
What should a solutions architect do to meet this requirement?

Options:
A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer
B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region
C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application
D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer

Answer: A

Explanation:

- A: Correct, multi-AZ Auto Scaling + ALB ensures HA for stateless app.

- B: Snapshots not HA.

- C: Latency-based routing across AZ not valid.

- D: Route 53 not for AZ balancing.

Question: 367
A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.
What should the company do to maximize its benefit?

Options:
A. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.
B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.
C. Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan.
D. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.

Answer: B

Explanation:

- A: Needs to be done at management account, not member.

- B: Correct, management account enables sharing.

- C: Migration not efficient.

- D: Reserved Instance Marketplace doesn't apply to Savings Plans.

Question: 368
A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.
Which solution will meet these requirements?

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

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

Answer: B

Explanation:

- A/C: WebSocket API not required here.

- B: Correct, REST API + VPC Link provides private access.

- D: Security group alone not enough.

Question: 369
A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested determines the access pattern on the S3 objects. The company cannot predict or control the access pattern. The company wants to reduce its S3 costs.
Which solution will meet these requirements?

Options:
A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA)
B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)
C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering
D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering

Answer: C

Explanation:

- A: Replication doesn't reduce storage cost.

- B: Lifecycle rules need known patterns.

- C: Correct, Intelligent-Tiering auto-optimizes cost without prediction.

- D: Inventory reports require manual action.

Question: 370
A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.
What should a solutions architect recommend to resolve this issue?

Options:
A. Create a NAT gateway and make it the destination of the subnet's route table
B. Create an internet gateway and make it the destination of the subnet's route table
C. Create a virtual private gateway and make it the destination of the subnet's route table
D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Answer: D

Explanation:

- A: NAT is for IPv4.

- B: Internet gateway allows inbound connections.

- C: Virtual private gateway is for VPN.

- D: Correct, egress-only gateway allows outbound IPv6 only.

Question: 371
A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.
Which solution will meet these requirements?

Options:
A. Enable S3 Intelligent-Tiering for the S3 bucket
B. Enable S3 Transfer Acceleration for the S3 bucket
C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC
D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC

Answer: C

Explanation:

- A: Storage class, not networking.

- B: Transfer Acceleration increases cost.

- C: Correct, gateway endpoint avoids internet cost.

- D: Interface endpoint unnecessary, higher cost.

Question: 372
A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.
Which method should the solutions architect select?

Options:
A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Answer: A

Explanation:

- A: Correct, DAX provides microsecond latency with minimal changes.

- B: Replicas not supported for DynamoDB.

- C: Adding RCUs won't reduce latency.

- D: Redis requires code changes, not minimal.

Question: 373
A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing, and the company is concerned about a potential increase in cost.
What should a solutions architect do?

Options:
A. Create an Amazon CloudFront distribution to cache static files at edge locations
B. Create an Amazon ElastiCache cluster. Connect the ALB to the ElastiCache cluster to serve cached files
C. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files
D. Create a second ALB in an alternative AWS Region. Route user traffic to the closest Region to minimize data transfer costs

Answer: A

Explanation:

- A: Correct, CloudFront caches static files, reduces cost.

- B: ElastiCache not suited for large static file delivery.

- C: WAF is for filtering, not caching.

- D: Adding ALB across Regions increases cost.

Question: 374
A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company's VPCs must communicate with all other VPCs across all Regions.
Which solution will meet these requirements with the LEAST amount of administrative effort?

Options:
A. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.
B. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.
D. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications

Answer: C

Explanation:

- A: Too complex with many connections.

- B: Direct Connect gateway is for hybrid, not cross-VPC.

- C: Correct, Transit Gateway + peering simplifies management.

- D: PrivateLink is for services, not full VPC-to-VPC comms.

Question: 375
A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target in each Availability Zone within a Region. A solutions architect wants to use AWS Backup to manage the replication to another Region.
Which solution will meet these requirements?

Options:
A. Amazon FSx for Windows File Server with a Multi-AZ deployment
B. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment
C. Amazon Elastic File System (Amazon EFS) with the Standard storage class
D. Amazon FSx for OpenZFS

Answer: C

Explanation:

- A: FSx for Windows not designed for multi-AZ Linux containers.

- B: NetApp ONTAP possible, but EFS is simpler and native.

- C: Correct, EFS with AWS Backup + multi-AZ targets is ideal.

- D: FSx for OpenZFS doesn't support full multi-region backup.

Question: 376

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

Which additional action is the MOST secure way to grant permissions to the new users?

Options:

A. Apply service control policies (SCPs) to manage access permissions

B. Create IAM roles that have least privilege permission. Attach the roles to the IAM groups

C. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups

D. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions

Answer: C

Explanation:

- A: SCPs are for accounts, not groups.

- B: Roles not attached to groups.

- C: Correct, IAM policies with least privilege attached to groups is best.

- D: Permissions boundary restricts, but doesn't assign.

Question: 377

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow"
        }
    ]
}
```

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

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

```
"Action": [
    "s3:*"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"
```

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

Answer: D

Explanation:

- A/B/C: Missing required actions.
- D: Correct, need explicit s3:DeleteObject permission.

Question: 378

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

Options:

A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.

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

C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.

D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Answer: B

Explanation:

- A: IAM permissions alone don't enforce immutability.

- B: Correct, Object Lock + versioning ensures no changes until retention ends.

- C: Lambda not reliable for security compliance.

- D: Object Lock must be at bucket level, not folder.

Question: 379

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

What should a solutions architect recommend to meet these requirements?

Options:

A. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones

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

C. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.

D. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones.

Answer: B

Explanation:

- A: Systems Manager not for infra provisioning.

- B: Correct, CloudFormation automates consistent infra deployment.

- C: AWS Config is auditing, not provisioning.

- D: Elastic Beanstalk not needed here.

Question: 380
A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.
Which capability should the solutions architect use to meet the compliance requirements?

Options:
A. AWS Key Management Service (AWS KMS)
B. VPC endpoint
C. Private subnet
D. Virtual private gateway

Answer: B

Explanation:

- A: KMS handles encryption, not network path.

- B: Correct, VPC endpoint keeps S3 traffic private.

- C: Private subnet alone doesn't stop public internet routing.

- D: Virtual private gateway is for VPN.

Question: 381
A company hosts a three-tier web application in the AWS Cloud. A Multi-AZ Amazon RDS for MySQL server forms the database layer. Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database. The data in the cache must always match the data in the database.
Which solution will meet these requirements?

Options:
A. Implement the lazy loading caching strategy
B. Implement the write-through caching strategy
C. Implement the adding TTL caching strategy
D. Implement the AWS AppConfig caching strategy

Answer: B

Explanation:

- A: Lazy loading only fetches on read, can cause stale data.

- B: Correct, write-through keeps cache updated.

- C: TTL doesn't guarantee sync with DB.

- D: AppConfig unrelated.

Question: 382
A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3 bucket. The company will store new data directly in Amazon S3.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket
B. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket
C. Use AWS Snowball to move the data to an S3 bucket
D. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket

Answer: B

Explanation:

- A: Manual and less efficient.

- B: Correct, DataSync automates encryption + transfer.

- C: Snowball unnecessary for 100 GB.

- D: VPN setup adds overhead.

Question: 383
A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Create an AWS Lambda function based on the container image of the job. Configure Amazon EventBridge to invoke the function every 10 minutes.
B. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes.
D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every 10 minutes.

Answer: C

Explanation:

- A: Lambda doesn't support Windows containers.

- B: Batch possible but more overhead.

- C: Correct, ECS Fargate scheduled tasks run container jobs cost-effectively.

- D: Windows task scheduler adds complexity.

Question: 384

A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)

Options:

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

B. Set up an Amazon Cognito identity pool. Configure AWS IAM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.

C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service.

D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.

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

Answer: AE

Explanation:

- A: Correct, Organizations + new accounts.

- B: Cognito not needed.

- C: SCP doesn't integrate authentication.

- D: Organizations doesn't authenticate via Directory Service directly.

- E: Correct, IAM Identity Center + directory integration.

Question: 385

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

What is the MOST cost-effective solution?

Options:

A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.

B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.

C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: A

Explanation:

- A: Correct, Glacier Expedited retrieval < 5 minutes.

- B: Glacier Standard retrieval takes hours.

- C: More expensive than Glacier.

- D: One Zone-IA not suitable for long-term archival.

Question: 386

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

Options:

A. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
B. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
C. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
D. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

Answer: A

Explanation:

- A: Correct, S3 + Fargate + RDS is simplest and cost-effective.

- B: CloudFront doesn't host static files, just caches.

- C: EKS adds complexity.

- D: EC2 Reserved Instances unnecessary.

Question: 387

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

Options:

A. Amazon FSx Multi-AZ deployments
B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes
C. Amazon Elastic File System (Amazon EFS) with multiple mount targets
D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points

Answer: C

Explanation:

- A: FSx not required here.

- B: EBS can't be shared across many instances.

- C: Correct, EFS multi-AZ + mount targets fits perfectly.

- D: Single mount target not HA.

Question: 388
A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts.
Which solution will meet these requirements?

Options:
A. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.
B. Attach an identity-based policy to deny access to the billing information to all users, including the root user.
C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU).
D. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.

Answer: C

Explanation:

- A: Doesn't block root access.

- B: Root can't be restricted by IAM policy.

- C: Correct, SCP blocks billing info even for root in member accounts.

- D: Consolidated billing removes features.

Question: 389
An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that some of the order messages were not received.
A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.
Which solution will meet these requirements with the LEAST development effort?

Options:
A. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.
B. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days.
D. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.

Answer: C

Explanation:

- A: Kinesis not necessary.

- B: Redesigns architecture.

- C: Correct, SNS DLQ + SQS retention is simplest.

- D: DynamoDB adds complexity.

Question: 390
A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table.
Which solution meets these requirements?

Options:
A. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.
B. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.
C. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.
D. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.

Answer: B

Explanation:

- A: EMR adds unnecessary complexity.

- B: Correct, DynamoDB export to S3 with PITR works seamlessly.

- C: Streams add coding complexity.

- D: Lambda requires custom jobs.

Question: 391
A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.
Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
B. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
C. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.
D. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.

Answer: A

Explanation:

- A: Correct, SQS Standard ensures at-least-once delivery + KMS encryption.

- B: FIFO unnecessary, costlier.

- C: Same as B.

- D: Overcomplicates with KMS key invocation.

Question: 392
A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts. The company wants to centrally restrict the creation of AWS resources in these accounts.
Which solution will meet these requirements with the LEAST development effort?

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

Answer: B

Explanation:

- A: Complex and indirect.

- B: Correct, SCPs centrally enforce limits.

- C: Reactive, not preventative.

- D: Service Catalog works but higher overhead.

Question: 393
A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.
The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.
Which combination of steps will meet these requirements? (Choose three.)

Options:
A. Use Amazon Comprehend to translate the audio recordings into English.
B. Use Amazon Lex to create the written sentiment analysis reports.
C. Use Amazon Polly to convert the audio recordings into text.
D. Use Amazon Transcribe to convert the audio recordings in any language into text.
E. Use Amazon Translate to translate text in any language to English.
F. Use Amazon Comprehend to create the sentiment analysis reports.

Answer: DEF

Explanation:

- D: Transcribe converts audio to text.

- E: Translate converts to English.

- F: Comprehend analyzes sentiment.

- A/B/C are wrong services.

Question: 394

A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.

The administrator is using an IAM role that has the following IAM policy attached:

What is the cause of the unsuccessful request?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

Options:

A. The EC2 instance has a resource-based policy with a Deny statement.

B. The principal has not been specified in the policy statement.

C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.

D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24.

Answer: D

Explanation:

- Policy likely had Condition restricting CIDR.

Question: 395

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

Which solution will meet these requirements?

Options:

A. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.

B. Configure Amazon S3 Inventory on the S3 bucket. Configure Amazon Athena to query the inventory.

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

D. Use Amazon S3 Select to run a report across the S3 bucket.

Answer: C

Explanation:

- A: Audit Manager doesn't scan data.

- B: Inventory doesn't analyze content.

- C: Correct, Macie detects PII + financial data.

- D: S3 Select queries structured content only.

Question: 396

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

Options:

A. Mount Amazon S3 as a file system to the on-premises servers.

B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.

C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.

D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.

E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Answer: BD

Explanation:

- B: File gateway for NFS.

- D: Volume gateway for block storage.

- A: S3 mounting not suitable.

- C/E: Not optimal here.

Question: 397
A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Answer: C

Explanation:

- A/B/D: Still incur NAT costs.

- C: Correct, S3 gateway endpoint avoids NAT charges.

Question: 398
A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object. The company needs to retain only the two most recent versions of the pictures. The company wants to reduce costs. The company has identified the S3 bucket as a large expense.
Which solution will reduce the S3 costs with the LEAST operational overhead?

Options:
A. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.
B. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions.
C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions.
D. Deactivate versioning on the S3 bucket and retain the two most recent versions.

Answer: A

Explanation:

- A: Correct, lifecycle rules automate deletion of older versions.

- B: Lambda adds coding effort.

- C: Batch Ops is more manual.

- D: Deactivating versioning prevents future versioning control.

Question: 399

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

Options:

A. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.
B. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.
C. Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the connection with another AWS account.
D. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS account.

Answer: D

Explanation:

- A/B/C: Doesn't reduce cost effectively.

- D: Correct, hosted DX connection from partner at smaller bandwidth.

Question: 400

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

Options:

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

Answer: AD

Explanation:

- A: Correct, DataSync keeps permissions intact.

- B/C/E: Using S3 as staging breaks Windows ACLs.

- D: Correct, Snowcone + DataSync works for migration with permissions.

Question 401:
A city has deployed a web application running on Amazon EC2 instances behind an Application Load Balancer (ALB). The application's users have reported sporadic performance, which appears to be related to DDoS attacks originating from random IP addresses. The city needs a solution that requires minimal configuration changes and provides an audit trail for the DDoS sources.
Which solution meets these requirements?

Options:
A.Enable an AWS WAF web ACL on the ALB, and configure rules to block traffic from unknown sources.
B.Subscribe to Amazon Inspector. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.
C.Subscribe to AWS Shield Advanced. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.
D.Create an Amazon CloudFront distribution for the application, and set the ALB as the origin. Enable an AWS WAF web ACL on the distribution, and configure rules to block traffic from unknown sources.

Answer: C

Explanation:

- Correct: Shield Advanced protects against DDoS, integrates with DRT, and provides visibility/audit trails.

- Option A is wrong because WAF blocks at L7, not full DDoS mitigation.

- Option B is wrong because Inspector is for vulnerability scanning, not DDoS.

- Option D is wrong because CloudFront + WAF adds latency and is not minimal change.

Question 402:
A company copies 200 TB of data from a recent ocean survey onto AWS Snowball Edge Storage Optimized devices. The company has a high performance computing (HPC) cluster that is hosted on AWS to look for oil and gas deposits. A solutions architect must provide the cluster with consistent sub-millisecond latency and high-throughput access to the data on the Snowball Edge Storage Optimized devices. The company is sending the devices back to AWS.
Which solution will meet these requirements?

Options:
A.Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an AWS Storage Gateway file gateway to use the S3 bucket. Access the file gateway from the HPC cluster instances.
B.Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an Amazon FSx for Lustre file system, and integrate it with the S3 bucket. Access the FSx for Lustre file system from the HPC cluster instances.
C.Create an Amazon S3 bucket and an Amazon Elastic File System (Amazon EFS) file system. Import the data into the S3 bucket. Copy the data from the S3 bucket to the EFS file system. Access the EFS file system from the HPC cluster instances.
D.Create an Amazon FSx for Lustre file system. Import the data directly into the FSx for Lustre file system. Access the FSx for Lustre file system from the HPC cluster instances.

Answer: D

Explanation:

- Correct: FSx for Lustre provides sub-millisecond latency and high throughput for HPC workloads.

- Option A is wrong because file gateway adds latency and overhead.

- Option B is wrong because importing into S3 first delays and complicates.

- Option C is wrong because EFS has higher latency than Lustre.

Question 403:
A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3.
Which solution meets these requirements and is MOST cost-effective?

Options:
A.Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
B.Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
C.Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.
D.Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Answer: B

Explanation:

- Correct: DataSync agent integrates with NFS servers and efficiently syncs to S3.

- Option A is wrong because Glue is for ETL, not file transfer.

- Option C is wrong because SFTP is not native for NFS backups.

- Option D is wrong because Direct Connect is costly and unnecessary.

Question 404:
An online video game company must maintain ultra-low latency for its game servers. The game servers run on Amazon EC2 instances. The company needs a solution that can handle millions of UDP internet traffic requests each second.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Configure an Application Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.
B.Configure a Gateway Load Balancer for the internet traffic. Specify the EC2 instances as the targets.
C.Configure a Network Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.
D.Launch an identical set of game servers on EC2 instances in separate AWS Regions. Route internet traffic to both sets of EC2 instances.

Answer: C

Explanation:

- Correct: NLB supports TCP/UDP at scale with ultra-low latency.

- Option A is wrong because ALB supports only HTTP/HTTPS.

- Option B is wrong because Gateway LB is for appliances, not game traffic.

- Option D is wrong because multi-region servers don't guarantee ultra-low latency.

Question 405:

A company runs a three-tier application in a VPC. The database tier uses an Amazon RDS for MySQL DB instance. The company plans to migrate the RDS for MySQL DB instance to an Amazon Aurora PostgreSQL DB cluster. The company needs a solution that replicates the data changes that happen during the migration to the new database.

Which combination of steps will meet these requirements? (Choose two.)

Options:

A.Use AWS Database Migration Service (AWS DMS) Schema Conversion to transform the database objects.

B.Use AWS Database Migration Service (AWS DMS) Schema Conversion to create an Aurora PostgreSQL read replica on the RDS for MySQL DB instance.

C.Configure an Aurora MySQL read replica for the RDS for MySQL DB instance.

D.Define an AWS Database Migration Service (AWS DMS) task with change data capture (CDC) to migrate the data.

E.Promote the Aurora PostgreSQL read replica to a standalone Aurora PostgreSQL DB cluster when the replica lag is zero.

Answer: AD

Explanation:

- Correct: Schema Conversion + DMS task with CDC ensures schema and ongoing replication.

- Option B is wrong because Aurora PostgreSQL cannot be a replica of MySQL.

- Option C is wrong because Aurora MySQL replica doesn't help migration to PostgreSQL.

- Option E is wrong because PostgreSQL replica promotion is irrelevant here.

Question 406:

A company hosts a database that runs on an Amazon RDS instance that is deployed to multiple Availability Zones. The company periodically runs a script against the database to report new entries that are added to the database. The script that runs against the database negatively affects the performance of a critical application. The company needs to improve application performance with minimal costs.

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

Options:

A.Add functionality to the script to identify the instance that has the fewest active connections. Configure the script to read from that instance to report the total new entries.

B.Create a read replica of the database. Configure the script to query only the read replica to report the total new entries.

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

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

Answer: B

Explanation:

- Correct: Read replica offloads read queries without affecting the main DB.

- Option A is wrong because multi-AZ doesn't allow direct reads from standby.

- Option C is wrong because manual export increases overhead.

- Option D is wrong because ElastiCache doesn't solve ad-hoc reporting needs.

Question 407:
A company is using an Application Load Balancer (ALB) to present its application to the internet. The company finds abnormal traffic access patterns across the application. A solutions architect needs to improve visibility into the infrastructure to help the company understand these abnormalities better.
What is the MOST operationally efficient solution that meets these requirements?

Options:
A.Create a table in Amazon Athena for AWS CloudTrail logs. Create a query for the relevant information.
B.Enable ALB access logging to Amazon S3. Create a table in Amazon Athena, and query the logs.
C.Enable ALB access logging to Amazon S3. Open each file in a text editor, and search each line for the relevant information.
D.Use Amazon EMR on a dedicated Amazon EC2 instance to directly query the ALB to acquire traffic access log information.

Answer: B

Explanation:

- Correct: ALB logs to S3 + Athena = scalable, efficient querying.

- Option A is wrong because CloudTrail tracks API calls, not traffic patterns.

- Option C is wrong because manual searching is inefficient.

- Option D is wrong because EMR is overkill for this use case.

Question 408:
A company wants to use NAT gateways in its AWS environment. The company's Amazon EC2 instances in private subnets must be able to connect to the public internet through the NAT gateways.
Which solution will meet these requirements?

Options:
A.Create public NAT gateways in the same private subnets as the EC2 instances.
B.Create private NAT gateways in the same private subnets as the EC2 instances.
C.Create public NAT gateways in public subnets in the same VPCs as the EC2 instances.
D.Create private NAT gateways in public subnets in the same VPCs as the EC2 instances.

Answer: C

Explanation:

- Correct: NAT gateways must be deployed in public subnets to provide outbound internet to private subnets.

- Option A is wrong because NAT can't be in private subnets.

- Option B is wrong because "private NAT" doesn't exist.

- Option D is wrong because public NAT must be in public subnets.

Question 409:
A company has an organization in AWS Organizations. The company runs Amazon EC2 instances across four AWS accounts in the root organizational unit (OU). There are three nonproduction accounts and one production account. The company wants to prohibit users from launching EC2 instances of a certain size in the nonproduction accounts. The company has created a service control policy (SCP) to deny access to launch instances that use the prohibited types.
Which solutions to deploy the SCP will meet these requirements? (Choose two.)

Options:
A.Attach the SCP to the root OU for the organization.
B.Attach the SCP to the three nonproduction Organizations member accounts.
C.Attach the SCP to the Organizations management account.
D.Create an OU for the production account. Attach the SCP to the OU. Move the production member account into the new OU.
E.Create an OU for the required accounts. Attach the SCP to the OU. Move the nonproduction member accounts into the new OU.

Answer: BE

Explanation:

- Correct: Attaching SCP directly to nonproduction accounts or an OU with only them enforces the restriction.

- Option A is wrong because applying at root would impact all accounts, including production.

- Option C is wrong because attaching to management account doesn't enforce on members.

- Option D is wrong because isolating production is unnecessary; nonproduction is the target.

Question 410:
A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.
Which solution meets these requirements?

Options:
A.Set up S3 bucket policies to allow access from a VPC endpoint.
B.Set up an IAM policy to grant read-write access to the S3 bucket.
C.Set up a NAT gateway to access resources outside the private subnet.
D.Set up an access key ID and a secret access key to access the S3 bucket.

Answer: A

Explanation:

- Correct: VPC endpoint ensures private access between EC2 and S3.

- Option B is wrong because IAM policies don't guarantee private network paths.

- Option C is wrong because NAT gateway uses internet, not private.

- Option D is wrong because access keys are not a network security solution.

Question 411:
An ecommerce company runs its application on AWS. The application uses an Amazon Aurora PostgreSQL cluster in Multi-AZ mode for the underlying database. During a recent promotional campaign, the application experienced heavy read load and write load. Users experienced timeout issues when they attempted to access the application. A solutions architect needs to make the application architecture more scalable and highly available.
Which solution will meet these requirements with the LEAST downtime?

Options:
A.Create an Amazon EventBridge rule that has the Aurora cluster as a source. Create an AWS Lambda function to log the state change events of the Aurora cluster. Add the Lambda function as a target for the EventBridge rule. Add additional reader nodes to fail over to.
B.Modify the Aurora cluster and activate the zero-downtime restart (ZDR) feature. Use Database Activity Streams on the cluster to track the cluster status.
C.Add additional reader instances to the Aurora cluster. Create an Amazon RDS Proxy target group for the Aurora cluster.
D.Create an Amazon ElastiCache for Redis cache. Replicate data from the Aurora cluster to Redis by using AWS Database Migration Service (AWS DMS) with a write-around approach.

Answer: C

Explanation:

- Correct: Aurora readers + RDS Proxy scale reads and improve availability.

- Option A is wrong because EventBridge logging doesn't fix scalability.

- Option B is wrong because ZDR just reduces restart downtime, not load handling.

- Option D is wrong because DMS is not designed for caching.

Question 412:
A company is designing a web application on AWS. The application will use a VPN connection between the company's existing data centers and the company's VPCs. The company uses Amazon Route 53 as its DNS service. The application must use private DNS records to communicate with the on-premises services from a VPC.
Which solution will meet these requirements in the MOST secure manner?

Options:
A.Create a Route 53 Resolver outbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC.
B.Create a Route 53 Resolver inbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC.
C.Create a Route 53 private hosted zone. Associate the private hosted zone with the VPC.
D.Create a Route 53 public hosted zone. Create a record for each service to allow service communication.

Answer: A

Explanation:

- Correct: Outbound endpoint + resolver rules allow secure queries to on-premises DNS.

- Option B is wrong because inbound endpoints are for on-premises → AWS queries.

- Option C is wrong because private hosted zones work for AWS, not hybrid DNS.

- Option D is wrong because public zones expose DNS externally.

Question 413:
A company is running a photo hosting service in the us-east-1 Region. The service enables users across multiple countries to upload and view photos. Some photos are heavily viewed for months, and others are viewed for less than a week. The application allows uploads of up to 20 MB for each photo. The service uses the photo metadata to determine which photos to display to each user.
Which solution provides the appropriate user access MOST cost-effectively?

Options:
A.Store the photos in Amazon DynamoDB. Turn on DynamoDB Accelerator (DAX) to cache frequently viewed items.
B.Store the photos in the Amazon S3 Intelligent-Tiering storage class. Store the photo metadata and its S3 location in DynamoDB.
C.Store the photos in the Amazon S3 Standard storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Use the object tags to keep track of metadata.
D.Store the photos in the Amazon S3 Glacier storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Glacier Deep Archive storage class. Store the photo metadata and its S3 location in Amazon OpenSearch Service.

Answer: B

Explanation:

- Correct: S3 Intelligent-Tiering automatically optimizes costs, DynamoDB stores metadata.

- Option A is wrong because DynamoDB is not designed for storing photos.

- Option C is wrong because lifecycle policies are static, not dynamic.

- Option D is wrong because Glacier retrieval latency is too high.

Question 414:
A company runs a highly available web application on Amazon EC2 instances behind an Application Load Balancer. The company uses Amazon CloudWatch metrics. As the traffic to the web application increases, some EC2 instances become overloaded with many outstanding requests. The CloudWatch metrics show that the number of requests processed and the time to receive the responses from some EC2 instances are both higher compared to other EC2 instances. The company does not want new requests to be forwarded to the EC2 instances that are already overloaded.
Which solution will meet these requirements?

Options:
A.Use the round robin routing algorithm based on the RequestCountPerTarget and ActiveConnectionCount CloudWatch metrics.
B.Use the least outstanding requests algorithm based on the RequestCountPerTarget and ActiveConnectionCount CloudWatch metrics.
C.Use the round robin routing algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.
D.Use the least outstanding requests algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.

Answer: B

Explanation:

- Correct: Least outstanding requests algorithm balances based on active connections.

- Option A is wrong because round robin doesn't consider load.

- Option C is wrong because round robin with metrics mismatch is irrelevant.

- Option D is wrong because TargetResponseTime is not optimal for load balancing.

Question 415:
A company uses Amazon EC2, AWS Fargate, and AWS Lambda to run multiple workloads in the company's AWS account. The company wants to fully make use of its Compute Savings Plans. The company wants to receive notification when coverage of the Compute Savings Plans drops.
Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Create a daily budget for the Savings Plans by using AWS Budgets. Configure the budget with a coverage threshold to send notifications to the appropriate email message recipients.
B.Create a Lambda function that runs a coverage report against the Savings Plans. Use Amazon Simple Email Service (Amazon SES) to email the report to the appropriate email message recipients.
C.Create an AWS Budgets report for the Savings Plans budget. Set the frequency to daily.
D.Create a Savings Plans alert subscription. Enable all notification options. Enter an email address to receive notifications.

Answer: A

Explanation:

- Correct: AWS Budgets with coverage threshold alerts is automated and efficient.

- Option B is wrong because custom Lambda adds unnecessary overhead.

- Option C is wrong because reports don't send real-time alerts.

- Option D is wrong because "Savings Plans alert subscription" is not a feature.

Question 416:
A company runs a real-time data ingestion solution on AWS. The solution consists of the most recent version of Amazon Managed Streaming for Apache Kafka (Amazon MSK). The solution is deployed in a VPC in private subnets across three Availability Zones. A solutions architect needs to redesign the data ingestion solution to be publicly available over the internet. The data in transit must also be encrypted.
Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Configure public subnets in the existing VPC. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.
B.Create a new VPC that has public subnets. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.
C.Deploy an Application Load Balancer (ALB) that uses private subnets. Configure an ALB security group inbound rule to allow inbound traffic from the VPC CIDR block for HTTPS protocol.
D.Deploy a Network Load Balancer (NLB) that uses private subnets. Configure an NLB listener for HTTPS communication over the internet.

Answer: A

Explanation:

- Correct: Deploying MSK in public subnets with TLS provides internet access securely.

- Option B is wrong because new VPC is unnecessary.

- Option C is wrong because ALB doesn't support Kafka protocol.

- Option D is wrong because NLB in private subnet won't allow public access.

Question 417:
A company wants to migrate an on-premises legacy application to AWS. The application ingests customer order files from an on-premises enterprise resource planning (ERP) system. The application then uploads the files to an SFTP server. The application uses a scheduled job that checks for order files every hour. The company already has an AWS account that has connectivity to the on-premises network. The new application on AWS must support integration with the existing ERP system. The new application must be secure and resilient and must use the SFTP protocol to process orders from the ERP system immediately.
Which solution will meet these requirements?

Options:
A.Create an AWS Transfer Family SFTP internet-facing server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use S3 Event Notifications to send s3:ObjectCreated:* events to the Lambda function.
B.Create an AWS Transfer Family SFTP internet-facing server in one Availability Zone. Use Amazon Elastic File System (Amazon EFS) storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.
C.Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon Elastic File System (Amazon EFS) storage. Create an AWS Step Functions state machine to process order files. Use Amazon EventBridge Scheduler to invoke the state machine to periodically check Amazon EFS for order files.
D.Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.

Answer: D

Explanation:

- Correct: Internal Transfer SFTP + S3 + Lambda workflow ensures secure and resilient order processing.

- Option A is wrong because internet-facing is not as secure.

- Option B is wrong because single AZ lacks high availability.

- Option C is wrong because periodic checks add delay instead of immediate processing.

Question 418:
A company's applications use Apache Hadoop and Apache Spark to process data on premises. The existing infrastructure is not scalable and is complex to manage. A solutions architect must design a scalable solution that reduces operational complexity. The solution must keep the data processing on premises.
Which solution will meet these requirements?

Options:
A.Use AWS Site-to-Site VPN to access the on-premises Hadoop Distributed File System (HDFS) data and application. Use an Amazon EMR cluster to process the data.
B.Use AWS DataSync to connect to the on-premises Hadoop Distributed File System (HDFS) cluster. Create an Amazon EMR cluster to process the data.
C.Migrate the Apache Hadoop application and the Apache Spark application to Amazon EMR clusters on AWS Outposts. Use the EMR clusters to process the data.
D.Use an AWS Snowball device to migrate the data to an Amazon S3 bucket. Create an Amazon EMR cluster to process the data.

Answer: C

Explanation:

- Correct: EMR on Outposts keeps data/processes on-premises, reduces complexity.

- Option A is wrong because Site-to-Site VPN doesn't solve compute locality.

- Option B is wrong because DataSync is for transfer, not local compute.

- Option D is wrong because Snowball migrates data, not keep on-premises.

Question 419:
A company is migrating a large amount of data from on-premises storage to AWS. Windows, Mac, and Linux based Amazon EC2 instances in the same AWS Region will access the data by using SMB and NFS storage protocols. The company will access a portion of the data routinely. The company will access the remaining data infrequently. The company needs to design a solution to host the data.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an Amazon Elastic File System (Amazon EFS) volume that uses EFS Intelligent-Tiering. Use AWS DataSync to migrate the data to the EFS volume.
B.Create an Amazon FSx for ONTAP instance. Create an FSx for ONTAP file system with a root volume that uses the auto tiering policy. Migrate the data to the FSx for ONTAP volume.
C.Create an Amazon S3 bucket that uses S3 Intelligent-Tiering. Migrate the data to the S3 bucket by using an AWS Storage Gateway Amazon S3 File Gateway.
D.Create an Amazon FSx for OpenZFS file system. Migrate the data to the new volume.

Answer: C

Explanation:

- Correct: S3 + File Gateway supports SMB/NFS access, with Intelligent-Tiering for cost optimization.

- Option A is wrong because EFS doesn't support SMB.

- Option B is wrong because FSx ONTAP works but higher overhead than File Gateway.

- Option D is wrong because OpenZFS lacks SMB support.

Question 420:
A manufacturing company runs its report generation application on AWS. The application generates each report in about 20 minutes. The application is built as a monolith that runs on a single Amazon EC2 instance. The application requires frequent updates to its tightly coupled modules. The application becomes complex to maintain as the company adds new features. Each time the company patches a software module, the application experiences downtime. Report generation must restart from the beginning after any interruptions. The company wants to redesign the application so that the application can be flexible, scalable, and gradually improved. The company wants to minimize application downtime.
Which solution will meet these requirements?

Options:
A.Run the application on AWS Lambda as a single function with maximum provisioned concurrency.
B.Run the application on Amazon EC2 Spot Instances as microservices with a Spot Fleet default allocation strategy.
C.Run the application on Amazon Elastic Container Service (Amazon ECS) as microservices with service auto scaling.
D.Run the application on AWS Elastic Beanstalk as a single application environment with an all-at-once deployment strategy.

Answer: C

Explanation:

- Correct: ECS microservices break monolith, scale independently, reduce downtime.

- Option A is wrong because a 20-min Lambda exceeds max runtime (15 min).

- Option B is wrong because Spot introduces interruptions.

- Option D is wrong because all-at-once Beanstalk deployments increase downtime.

Question 421:
A company wants to rearchitect a large-scale web application to a serverless microservices architecture. The application uses Amazon EC2 instances and is written in Python. The company selected one component of the web application to test as a microservice. The component supports hundreds of requests each second. The company wants to create and test the microservice on an AWS solution that supports Python. The solution must also scale automatically and require minimal infrastructure and minimal operational support.
Which solution will meet these requirements?

Options:
A.Use a Spot Fleet with auto scaling of EC2 instances that run the most recent Amazon Linux operating system.
B.Use an AWS Elastic Beanstalk web server environment that has high availability configured.
C.Use Amazon Elastic Kubernetes Service (Amazon EKS). Launch Auto Scaling groups of self-managed EC2 instances.
D.Use an AWS Lambda function that runs custom developed code.

Answer: D

Explanation:

- Correct: Lambda supports Python, scales automatically, minimal ops.

- Option A is wrong because EC2 fleet is high maintenance.

- Option B is wrong because Beanstalk still manages servers.

- Option C is wrong because EKS with EC2 adds infra overhead.

Question 422:
A company has an AWS Direct Connect connection from its on-premises location to an AWS account. The AWS account has 30 different VPCs in the same AWS Region. The VPCs use private virtual interfaces (VIFs). Each VPC has a CIDR block that does not overlap with other networks under the company's control. The company wants to centrally manage the networking architecture while still allowing each VPC to communicate with all other VPCs and on-premises networks.
Which solution will meet these requirements with the LEAST amount of operational overhead?

Options:
A.Create a transit gateway, and associate the Direct Connect connection with a new transit VIF. Turn on the transit gateway's route propagation feature.
B.Create a Direct Connect gateway. Recreate the private VIFs to use the new gateway. Associate each VPC by creating new virtual private gateways.
C.Create a transit VPC. Connect the Direct Connect connection to the transit VPC. Create a peering connection between all other VPCs in the Region. Update the route tables.
D.Create AWS Site-to-Site VPN connections from on premises to each VPC. Ensure that both VPN tunnels are UP for each connection. Turn on the route propagation feature.

Answer: A

Explanation:

- Correct: Transit Gateway + transit VIF centralizes VPC and on-premises connectivity with least overhead.

- Option B is wrong because recreating 30 VIFs increases effort.

- Option C is wrong because peering doesn't scale to 30+ VPCs.

- Option D is wrong because VPN for each VPC adds complexity.

Question 423:
A company has applications that run on Amazon EC2 instances. The EC2 instances connect to Amazon RDS databases by using an IAM role that has associated policies. The company wants to use AWS Systems Manager to patch the EC2 instances without disrupting the running applications.
Which solution will meet these requirements?

Options:
A.Create a new IAM role. Attach the AmazonSSMManagedInstanceCore policy to the new IAM role. Attach the new IAM role to the EC2 instances and the existing IAM role.
B.Create an IAM user. Attach the AmazonSSMManagedInstanceCore policy to the IAM user. Configure Systems Manager to use the IAM user to manage the EC2 instances.
C.Enable Default Host Configuration Management in Systems Manager to manage the EC2 instances.
D.Remove the existing policies from the existing IAM role. Add the AmazonSSMManagedInstanceCore policy to the existing IAM role.

Answer: A

Explanation:

- Correct: Attaching SSM core policy via a new IAM role allows patching while preserving existing role policies.

- Option B is wrong because SSM doesn't manage EC2 via IAM users.

- Option C is wrong because no such feature exists.

- Option D is wrong because removing policies would break DB access.

Question 424:
A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS) and the Kubernetes Horizontal Pod Autoscaler. The workload is not consistent throughout the day. A solutions architect notices that the number of nodes does not automatically scale out when the existing nodes have reached maximum capacity in the cluster, which causes performance issues.
Which solution will resolve this issue with the LEAST administrative overhead?

Options:
A.Scale out the nodes by tracking the memory usage.
B.Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.
C.Use an AWS Lambda function to resize the EKS cluster automatically.
D.Use an Amazon EC2 Auto Scaling group to distribute the workload.

Answer: B

Explanation:

- Correct: Cluster Autoscaler integrates with EKS and Auto Scaling to scale nodes automatically.

- Option A is wrong because manual tracking is not automated.

- Option C is wrong because custom Lambda adds overhead.

- Option D is wrong because ASG alone doesn't manage Kubernetes pod scheduling.

Question 425:
A company maintains about 300 TB in Amazon S3 Standard storage month after month. The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application. The number and size of S3 objects remain constant, but the company's S3 storage costs are increasing each month.
How should a solutions architect reduce costs in this situation?

Options:
A.Switch from multipart uploads to Amazon S3 Transfer Acceleration.
B.Enable an S3 Lifecycle policy that deletes incomplete multipart uploads.
C.Configure S3 inventory to prevent objects from being archived too quickly.
D.Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3.

Answer: B

Explanation:

- Correct: Incomplete multipart uploads accumulate and add storage cost, lifecycle deletes them.

- Option A is wrong because Transfer Acceleration is for faster uploads, not cost.

- Option C is wrong because inventory doesn't manage incomplete uploads.

- Option D is wrong because CloudFront doesn't reduce S3 stored object count.

Question 426:
A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations. The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.
What should a solutions architect do to improve the performance of the data tier?

Options:
A.Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
B.Migrate from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards.
C.Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
D.Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Answer: D

Explanation:

- Correct: ElastiCache for Redis provides rapid read/write updates with low latency.

- Option A is wrong because Multi-AZ improves availability, not performance.

- Option B is wrong because OpenSearch is for search/analytics, not rapid updates.

- Option C is wrong because DAX is for DynamoDB, not RDS.

Question 427:
A company stores critical data in Amazon DynamoDB tables in the company's AWS account. An IT administrator accidentally deleted a DynamoDB table. The deletion caused a significant loss of data and disrupted the company's operations. The company wants to prevent this type of disruption in the future.
Which solution will meet this requirement with the LEAST operational overhead?

Options:
A.Configure a trail in AWS CloudTrail. Create an Amazon EventBridge rule for delete actions. Create an AWS Lambda function to automatically restore deleted DynamoDB tables.
B.Create a backup and restore plan for the DynamoDB tables. Recover the DynamoDB tables manually.
C.Configure deletion protection on the DynamoDB tables.
D.Enable point-in-time recovery on the DynamoDB tables.

Answer: C

Explanation:

- Correct: Deletion protection prevents accidental table deletion.

- Option A is wrong because it adds operational complexity.

- Option B is wrong because recovery is manual and time-consuming.

- Option D is wrong because PITR recovers data, but the table could still be deleted.

Question 428:
A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.
How can these requirements be met?

Options:
A.Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
B.Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
C.Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
D.Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Answer: C

Explanation:

- Correct: Stored volumes keep full local copy for immediate retrieval, while backing up to S3.

- Option A is wrong because Glacier incurs retrieval costs/delay.

- Option B is wrong because cached volumes keep only frequently used data locally.

- Option D is wrong because Direct Connect doesn't solve storage retrieval.

Question 429:
A company runs a three-tier web application in a VPC across multiple Availability Zones. Amazon EC2 instances run in an Auto Scaling group for the application tier. The company needs to make an automated scaling plan that will analyze each resource's daily and weekly historical workload trends. The configuration must scale resources appropriately according to both the forecast and live changes in utilization.
Which scaling strategy should a solutions architect recommend to meet these requirements?

Options:
A.Implement dynamic scaling with step scaling based on average CPU utilization from the EC2 instances.
B.Enable predictive scaling to forecast and scale. Configure dynamic scaling with target tracking.
C.Create an automated scheduled scaling action based on the traffic patterns of the web application.
D.Set up a simple scaling policy. Increase the cooldown period based on the EC2 instance startup time.

Answer: B

Explanation:

- Correct: Predictive + dynamic scaling uses trends and live data together.

- Option A is wrong because step scaling reacts only to real-time, not forecasts.

- Option C is wrong because scheduled scaling can't adapt to unexpected spikes.

- Option D is wrong because cooldown adjustment doesn't meet forecasting needs.

Question 430:
A package delivery company has an application that uses Amazon EC2 instances and an Amazon Aurora MySQL DB cluster. As the application becomes more popular, EC2 instance usage increases only slightly. DB cluster usage increases at a much faster rate. The company adds a read replica, which reduces the DB cluster usage for a short period of time. However, the load continues to increase. The operations that cause the increase in DB cluster usage are all repeated read statements that are related to delivery details. The company needs to alleviate the effect of repeated reads on the DB cluster.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Implement an Amazon ElastiCache for Redis cluster between the application and the DB cluster.
B.Add an additional read replica to the DB cluster.
C.Configure Aurora Auto Scaling for the Aurora read replicas.
D.Modify the DB cluster to have multiple writer instances.

Answer: A

Explanation:

- Correct: ElastiCache caches repeated reads, reducing DB load cost-effectively.

- Option B is wrong because replicas still stress Aurora with repeated reads.

- Option C is wrong because scaling replicas doesn't reduce redundant queries.

- Option D is wrong because multi-writer is costly and unnecessary for read-heavy load.

Question 431:
A company has an application that uses an Amazon DynamoDB table for storage. A solutions architect discovers that many requests to the table are not returning the latest data. The company's users have not reported any other issues with database performance. Latency is in an acceptable range.
Which design change should the solutions architect recommend?

Options:
A.Add read replicas to the table.
B.Use a global secondary index (GSI).
C.Request strongly consistent reads for the table.
D.Request eventually consistent reads for the table.

Answer: C

Explanation:

- Correct: Strongly consistent reads return the latest data.

- Option A is wrong because DynamoDB doesn't use read replicas.

- Option B is wrong because GSI doesn't fix consistency.

- Option D is wrong because eventual consistency already causes stale data.

Question 432:
A company has deployed its application on Amazon EC2 instances with an Amazon RDS database. The company used the principle of least privilege to configure the database access credentials. The company's security team wants to protect the application and the database from SQL injection and other web-based attacks.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use security groups and network ACLs to secure the database and application servers.
B.Use AWS WAF to protect the application. Use RDS parameter groups to configure the security settings.
C.Use AWS Network Firewall to protect the application and the database.
D.Use different database accounts in the application code for different functions. Avoid granting excessive privileges to the database users.

Answer: B

Explanation:

- Correct: WAF blocks SQL injection/web exploits with minimal setup.

- Option A is wrong because NACLs/SGs don't block SQL injection.

- Option C is wrong because Network Firewall is for network traffic, not app layer.

- Option D is wrong because least privilege already applied, but no web protection.

Question 433:
An ecommerce company runs applications in AWS accounts that are part of an organization in AWS Organizations. The applications run on Amazon Aurora PostgreSQL databases across all the accounts. The company needs to prevent malicious activity and must identify abnormal failed and incomplete login attempts to the databases.
Which solution will meet these requirements in the MOST operationally efficient way?

Options:
A.Attach service control policies (SCPs) to the root of the organization to identify the failed login attempts.
B.Enable the Amazon RDS Protection feature in Amazon GuardDuty for the member accounts of the organization.
C.Publish the Aurora general logs to a log group in Amazon CloudWatch Logs. Export the log data to a central Amazon S3 bucket.
D.Publish all the Aurora PostgreSQL database events in AWS CloudTrail to a central Amazon S3 bucket.

Answer: B

Explanation:

- Correct: GuardDuty RDS Protection detects malicious login behavior with minimal ops.

- Option A is wrong because SCPs control actions, not monitor logins.

- Option C is wrong because log shipping requires manual detection setup.

- Option D is wrong because CloudTrail doesn't capture failed DB login attempts.

Question 434:
A company has an AWS Direct Connect connection from its corporate data center to its VPC in the us-east-1 Region. The company recently acquired a corporation that has several VPCs and a Direct Connect connection between its on-premises data center and the eu-west-2 Region. The CIDR blocks for the VPCs of the company and the corporation do not overlap. The company requires connectivity between two Regions and the data centers. The company needs a solution that is scalable while reducing operational overhead.
What should a solutions architect do to meet these requirements?

Options:
A.Set up inter-Region VPC peering between the VPC in us-east-1 and the VPCs in eu-west-2.
B.Create private virtual interfaces from the Direct Connect connection in us-east-1 to the VPCs in eu-west-2.
C.Establish VPN appliances in a fully meshed VPN network hosted by Amazon EC2. Use AWS VPN CloudHub to send and receive data between the data centers and each VPC.
D.Connect the existing Direct Connect connection to a Direct Connect gateway. Route traffic from the virtual private gateways of the VPCs in each Region to the Direct Connect gateway.

Answer: D

Explanation:

- Correct: Direct Connect gateway enables multi-region VPC + data center connectivity.

- Option A is wrong because VPC peering doesn't scale well.

- Option B is wrong because private VIFs cannot connect across regions directly.

- Option C is wrong because VPN mesh adds high overhead.

Question 435:
A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.
What should the solutions architect do to meet these requirements?

Options:
A.Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
B.Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
C.Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
D.Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer: A

Explanation:

- Correct: Kinesis Data Streams preserves order, Lambda processes, DynamoDB stores HA data with low ops.

- Option B is wrong because EC2 adds high management overhead.

- Option C is wrong because SNS doesn't guarantee message ordering.

- Option D is wrong because SQS doesn't preserve strict ordering by default.

Question 436:
A company has multiple AWS accounts with applications deployed in the us-west-2 Region. Application logs are stored within Amazon S3 buckets in each account. The company wants to build a centralized log analysis solution that uses a single S3 bucket. Logs must not leave us-west-2, and the company wants to incur minimal operational overhead.
Which solution meets these requirements and is MOST cost-effective?

Options:
A.Create an S3 Lifecycle policy that copies the objects from one of the application S3 buckets to the centralized S3 bucket.
B.Use S3 Same-Region Replication to replicate logs from the S3 buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
C.Write a script that uses the PutObject API operation every day to copy the entire contents of the buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
D.Write AWS Lambda functions in these accounts that are triggered every time logs are delivered to the S3 buckets (s3:ObjectCreated:* event). Copy the logs to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

Answer: B

Explanation:

- Correct: S3 Same-Region Replication automates centralized storage with low ops.

- Option A is wrong because Lifecycle can't copy across buckets.

- Option C is wrong because custom script adds overhead.

- Option D is wrong because Lambda-based copying increases complexity.

Question 437:
A company has an application that delivers on-demand training videos to students around the world. The application also allows authorized content developers to upload videos. The data is stored in an Amazon S3 bucket in the us-east-2 Region. The company has created an S3 bucket in the eu-west-2 Region and an S3 bucket in the ap-southeast-1 Region. The company wants to replicate the data to the new S3 buckets. The company needs to minimize latency for developers who upload videos and students who stream videos near eu-west-2 and ap-southeast-1.
Which combination of steps will meet these requirements with the FEWEST changes to the application? (Choose two.)

Options:
A.Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the us-east-2 S3 bucket to the ap-southeast-1 S3 bucket.
B.Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the eu-west-2 S3 bucket to the ap-southeast-1 S3 bucket.
C.Configure two-way (bidirectional) replication among the S3 buckets that are in all three Regions.
D.Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming. Do not modify the application for video uploads.
E.Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming and uploads.

Answer: CE

Explanation:

- Correct: Multi-Region Access Point optimizes latency for both uploads and streaming, and two-way replication ensures data consistency across regions.

- Option A is wrong because one-way replication doesn't sync between remote regions.

- Option B is wrong because chaining replications adds latency/complexity.

- Option D is wrong because only streaming is optimized, not uploads.

Question 438:

A company has a new mobile app. Anywhere in the world, users can see local news on topics they choose. Users also can post photos and videos from inside the app. Users access content often in the first minutes after the content is posted. New content quickly replaces older content, and then the older content disappears. The local nature of the news means that users consume 90% of the content within the AWS Region where it is uploaded.

Which solution will optimize the user experience by providing the LOWEST latency for content uploads?

Options:

A.Upload and store content in Amazon S3. Use Amazon CloudFront for the uploads.

B.Upload and store content in Amazon S3. Use S3 Transfer Acceleration for the uploads.

C.Upload content to Amazon EC2 instances in the Region that is closest to the user. Copy the data to Amazon S3.

D.Upload and store content in Amazon S3 in the Region that is closest to the user. Use multiple distributions of Amazon CloudFront.

Answer: B

Explanation:

- Correct: S3 Transfer Acceleration speeds up uploads globally with low latency.

- Option A is wrong because CloudFront accelerates downloads, not uploads.

- Option C is wrong because EC2 adds unnecessary complexity.

- Option D is wrong because multiple CloudFront distributions don't speed uploads.

Question 439:

A company is building a new application that uses serverless architecture. The architecture will consist of an Amazon API Gateway REST API and AWS Lambda functions to manage incoming requests. The company wants to add a service that can send messages received from the API Gateway REST API to multiple target Lambda functions for processing. The service must offer message filtering that gives the target Lambda functions the ability to receive only the messages the functions need.

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

Options:

A.Send the requests from the API Gateway REST API to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure the target Lambda functions to poll the different SQS queues.

B.Send the requests from the API Gateway REST API to Amazon EventBridge. Configure EventBridge to invoke the target Lambda functions.

C.Send the requests from the API Gateway REST API to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Configure Amazon MSK to publish the messages to the target Lambda functions.

D.Send the requests from the API Gateway REST API to multiple Amazon Simple Queue Service (Amazon SQS) queues. Configure the target Lambda functions to poll the different SQS queues.

Answer: A

Explanation:

- Correct: SNS + SQS fan-out with filtering allows selective delivery to Lambda.

- Option B is wrong because EventBridge lacks built-in fan-out filtering at scale.

- Option C is wrong because MSK is heavy for this need.

- Option D is wrong because direct SQS queues require more management.

Question 440:
A company migrated millions of archival files to Amazon S3. A solutions architect needs to implement a solution that will encrypt all the archival data by using a customer-provided key. The solution must encrypt existing unencrypted objects and future objects.
Which solution will meet these requirements?

Options:
A.Create a list of unencrypted objects by filtering an Amazon S3 Inventory report. Configure an S3 Batch Operations job to encrypt the objects from the list with a server-side encryption with a customer-provided key (SSE-C). Configure the S3 default encryption feature to use a server-side encryption with a customer-provided key (SSE-C).
B.Use S3 Storage Lens metrics to identify unencrypted S3 buckets. Configure the S3 default encryption feature to use a server-side encryption with AWS KMS keys (SSE-KMS).
C.Create a list of unencrypted objects by filtering the AWS usage report for Amazon S3. Configure an AWS Batch job to encrypt the objects from the list with a server-side encryption with AWS KMS keys (SSE-KMS). Configure the S3 default encryption feature to use a server-side encryption with AWS KMS keys (SSE-KMS).
D.Create a list of unencrypted objects by filtering the AWS usage report for Amazon S3. Configure the S3 default encryption feature to use a server-side encryption with a customer-provided key (SSE-C).

Answer: A

Explanation:

- Correct: Inventory + Batch Operations + SSE-C ensures both past and future encryption with customer keys.

- Option B is wrong because it uses SSE-KMS, not customer-provided keys.

- Option C is wrong because it also uses SSE-KMS.

- Option D is wrong because existing objects would remain unencrypted.

Question 441:
The DNS provider that hosts a company's domain name records is experiencing outages that cause service disruption for a website running on AWS. The company needs to migrate to a more resilient managed DNS service and wants the service to run on AWS.
What should a solutions architect do to rapidly migrate the DNS hosting service?

Options:
A.Create an Amazon Route 53 public hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider.
B.Create an Amazon Route 53 private hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider.
C.Create a Simple AD directory in AWS. Enable zone transfer between the DNS provider and AWS Directory Service for Microsoft Active Directory for the domain records.
D.Create an Amazon Route 53 Resolver inbound endpoint in the VPC. Specify the IP addresses that the provider's DNS will forward DNS queries to. Configure the provider's DNS to forward DNS queries for the domain to the IP addresses that are specified in the inbound endpoint.

Answer: A

Explanation:

- Correct: Route 53 public hosted zone replaces external DNS provider quickly.

- Option B is wrong because private hosted zones are not for public websites.

- Option C is wrong because Simple AD is unrelated to DNS hosting.

- Option D is wrong because Resolver inbound is for hybrid DNS queries.

Question 442:
A company is building an application on AWS that connects to an Amazon RDS database. The company wants to manage the application configuration and to securely store and retrieve credentials for the database and other services.
Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A.Use AWS AppConfig to store and manage the application configuration. Use AWS Secrets Manager to store and retrieve the credentials.
B.Use AWS Lambda to store and manage the application configuration. Use AWS Systems Manager Parameter Store to store and retrieve the credentials.
C.Use an encrypted application configuration file. Store the file in Amazon S3 for the application configuration. Create another S3 file to store and retrieve the credentials.
D.Use AWS AppConfig to store and manage the application configuration. Use Amazon RDS to store and retrieve the credentials.

Answer: A

Explanation:

- Correct: AppConfig + Secrets Manager is managed and secure with low ops.

- Option B is wrong because Lambda isn't config storage.

- Option C is wrong because S3 isn't secure for secrets.

- Option D is wrong because RDS isn't for credentials storage.

Question 443:
To meet security requirements, a company needs to encrypt all of its application data in transit while communicating with an Amazon RDS MySQL DB instance. A recent security audit revealed that encryption at rest is enabled using AWS Key Management Service (AWS KMS), but data in transit is not enabled.
What should a solutions architect do to satisfy the security requirements?

Options:
A.Enable IAM database authentication on the database.
B.Provide self-signed certificates. Use the certificates in all connections to the RDS instance.
C.Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption enabled.
D.Download AWS-provided root certificates. Provide the certificates in all connections to the RDS instance.

Answer: D

Explanation:

- Correct: AWS RDS requires TLS with AWS-provided certificates for in-transit encryption.

- Option A is wrong because IAM auth is unrelated to in-transit encryption.

- Option B is wrong because self-signed certs don't meet AWS security standard.

- Option C is wrong because snapshot restore affects rest, not transit.

Question 444:
A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancing (ELB) load balancer. However, many of the web service clients can only reach IP addresses authorized on their firewalls.
What should a solutions architect recommend to meet the clients' needs?

Options:
A.A Network Load Balancer with an associated Elastic IP address.
B.An Application Load Balancer with an associated Elastic IP address.
C.An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.
D.An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer: A

Explanation:

- Correct: NLB supports static Elastic IPs, allowing clients to whitelist fixed addresses.

- Option B is wrong because ALB doesn't support static EIPs.

- Option C is wrong because Route 53 A record resolves DNS, not IP whitelisting.

- Option D is wrong because proxy EC2 adds unnecessary overhead.

Question 445:
A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.
What should be done to secure the root user?

Options:
A.Create IAM users for daily administrative tasks. Disable the root user.
B.Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
C.Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
D.Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Answer: B

Explanation:

- Correct: MFA + IAM users secures the root account properly.

- Option A is wrong because root cannot be disabled.

- Option C is wrong because root access keys are insecure.

- Option D is wrong because root should never be used daily.

Question 446:
A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.
Which combination of network solutions will meet these requirements? (Choose two.)

Options:
A.Enable and configure enhanced networking on each EC2 instance.
B.Group the EC2 instances in separate accounts.
C.Run the EC2 instances in a cluster placement group.
D.Attach multiple elastic network interfaces to each EC2 instance.
E.Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Answer: AC

Explanation:

- Correct: Enhanced networking + cluster placement group provides lowest latency.

- Option B is wrong because separate accounts don't reduce latency.

- Option D is wrong because multiple ENIs don't reduce latency.

- Option E is wrong because EBS optimization affects storage, not network latency.

Question 447:
A financial services company wants to shut down two data centers and migrate more than 100 TB of data to AWS. The data has an intricate directory structure with millions of small files stored in deep hierarchies of subfolders. Most of the data is unstructured, and the company's file storage consists of SMB-based storage types from multiple vendors. The company does not want to change its applications to access the data after migration.
What should a solutions architect do to meet these requirements with the LEAST operational overhead?

Options:
A.Use AWS Direct Connect to migrate the data to Amazon S3.
B.Use AWS DataSync to migrate the data to Amazon FSx for Lustre.
C.Use AWS DataSync to migrate the data to Amazon FSx for Windows File Server.
D.Use AWS Direct Connect to migrate the data on-premises file storage to an AWS Storage Gateway volume gateway.

Answer: C

Explanation:

- Correct: FSx for Windows File Server supports SMB and DataSync migrates efficiently.

- Option A is wrong because S3 doesn't support SMB directly.

- Option B is wrong because FSx for Lustre is for HPC workloads.

- Option D is wrong because Storage Gateway isn't best for 100TB migration.

Question 448:

A company uses an organization in AWS Organizations to manage AWS accounts that contain applications. The company sets up a dedicated monitoring member account in the organization. The company wants to query and visualize observability data across the accounts by using Amazon CloudWatch.

Which solution will meet these requirements?

Options:

A.Enable CloudWatch cross-account observability for the monitoring account. Deploy an AWS CloudFormation template provided by the monitoring account in each AWS account to share the data with the monitoring account.

B.Set up service control policies (SCPs) to provide access to CloudWatch in the monitoring account under the Organizations root organizational unit (OU).

C.Configure a new IAM user in the monitoring account. In each AWS account, configure an IAM policy to have access to query and visualize the CloudWatch data in the account. Attach the new IAM policy to the new IAM user.

D.Create a new IAM user in the monitoring account. Create cross-account IAM policies in each AWS account. Attach the IAM policies to the new IAM user.

Answer: A

Explanation:

- Correct: CloudWatch cross-account observability centralizes monitoring with low ops.

- Option B is wrong because SCPs control services, not observability data sharing.

- Option C is wrong because IAM user-based access is manual.

- Option D is wrong because cross-account IAM policies add complexity.

Question 449:

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

Options:

A.Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.

B.Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.

C.Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

D.Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer: B

Explanation:

- Correct: WAF IP block protects at edge, preventing traffic from reaching ALB/EC2.

- Option A is wrong because CloudFront doesn't use NACLs.

- Option C is wrong because NACLs are at subnet level, not fine-grained.

- Option D is wrong because SG changes don't block via CloudFront/WAF path.

Question 450:
A company sets up an organization in AWS Organizations that contains 10 AWS accounts. A
solutions architect must design a solution to provide access to the accounts for several
thousand employees. The company has an existing identity provider (IdP). The company wants
to use the existing IdP for authentication to AWS.
Which solution will meet these requirements?

Options:
A.Create IAM users for the employees in the required AWS accounts. Connect IAM users to the
existing IdP. Configure federated authentication for the IAM users.
B.Set up AWS account root users with user email addresses and passwords that are
synchronized from the existing IdP.
C.Configure AWS IAM Identity Center (AWS Single Sign-On). Connect IAM Identity Center to the
existing IdP. Provision users and groups from the existing IdP.
D.Use AWS Resource Access Manager (AWS RAM) to share access to the AWS accounts with
the users in the existing IdP.

Answer: C

Explanation:

- Correct: IAM Identity Center integrates with IdP for centralized authentication/SSO.

- Option A is wrong because IAM users don't scale to thousands of employees.

- Option B is wrong because root user must never be used.

- Option D is wrong because RAM shares resources, not authentication.

Question 451:
A solutions architect is designing an AWS Identity and Access Management (IAM) authorization
model for a company's AWS account. The company has designated five specific employees to
have full access to AWS services and resources in the AWS account. The solutions architect
has created an IAM user for each of the five designated employees and has created an IAM user
group.
Which solution will meet these requirements?

Options:
A.Attach the AdministratorAccess resource-based policy to the IAM user group. Place each of
the five designated employee IAM users in the IAM user group.
B.Attach the SystemAdministrator identity-based policy to the IAM user group. Place each of
the five designated employee IAM users in the IAM user group.
C.Attach the AdministratorAccess identity-based policy to the IAM user group. Place each of
the five designated employee IAM users in the IAM user group.
D.Attach the SystemAdministrator resource-based policy to the IAM user group. Place each of
the five designated employee IAM users in the IAM user group.

Answer: C

Explanation:

- Correct: IAM groups use identity-based policies. AdministratorAccess policy grants full
  permissions.

- Option A is wrong because resource-based policies attach to resources, not groups.

- Option B is wrong because there's no managed policy called SystemAdministrator.

- Option D is wrong because IAM groups cannot use resource-based policies.

Question 452:
A company has a multi-tier payment processing application that is based on virtual machines (VMs). The communication between the tiers occurs asynchronously through a third-party middleware solution that guarantees exactly-once delivery. The company needs a solution that requires the least amount of infrastructure management. The solution must guarantee exactly-once delivery for application messaging.
Which combination of actions will meet these requirements? (Choose two.)

Options:
A.Use AWS Lambda for the compute layers in the architecture.
B.Use Amazon EC2 instances for the compute layers in the architecture.
C.Use Amazon Simple Notification Service (Amazon SNS) as the messaging component between the compute layers.
D.Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the messaging component between the compute layers.
E.Use containers that are based on Amazon Elastic Kubernetes Service (Amazon EKS) for the compute layers in the architecture.

Answer: AD

Explanation:

- Correct: Lambda minimizes infrastructure management. SQS FIFO guarantees exactly-once message delivery.

- Option B is wrong because EC2 requires infrastructure management.

- Option C is wrong because SNS does not provide exactly-once delivery.

- Option E is wrong because EKS adds unnecessary operational overhead.

Question 453:
A company has a nightly batch processing routine that analyzes report files that an on-premises file system receives daily through SFTP. The company wants to move the solution to the AWS Cloud. The solution must be highly available and resilient. The solution also must minimize operational effort.
Which solution meets these requirements?

Options:
A.Deploy AWS Transfer for SFTP and an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Amazon EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.
B.Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic Block Store (Amazon EBS) volume for storage. Use an Auto Scaling group with the minimum number of instances and desired number of instances set to 1.
C.Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Auto Scaling group with the minimum number of instances and desired number of instances set to 1.
D.Deploy AWS Transfer for SFTP and an Amazon S3 bucket for storage. Modify the application to pull the batch files from Amazon S3 to an Amazon EC2 instance for processing. Use an EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.

Answer: D

Explanation:

- Correct: Transfer Family + S3 provides serverless, HA SFTP with minimal ops.

- Option A is wrong because EFS adds cost and complexity for batch jobs.

- Option B is wrong because EC2 single instance is not resilient.

- Option C is wrong because EC2 + EFS still adds operational burden.

Question 454:
A company has users all around the world accessing its HTTP-based application deployed on Amazon EC2 instances in multiple AWS Regions. The company wants to improve the availability and performance of the application. The company also wants to protect the application against common web exploits that may affect availability, compromise security, or consume excessive resources. Static IP addresses are required.
What should a solutions architect recommend to accomplish this?

Options:
A.Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an accelerator using AWS Global Accelerator and register the NLBs as endpoints.
B.Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Deploy AWS WAF on the ALBs. Create an accelerator using AWS Global Accelerator and register the ALBs as endpoints.
C.Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
D.Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs. Deploy AWS WAF on the CloudFront distribution.

Answer: D

Explanation:

- Correct: CloudFront + ALB + WAF improves global performance, adds protection, and supports static IPs via CloudFront.

- Option A is wrong because WAF cannot attach to NLB.

- Option B is wrong because Global Accelerator with ALB does not add WAF integration.

- Option C is wrong because WAF cannot attach to NLB.

Question 455:
A company's data platform uses an Amazon Aurora MySQL database. The database has multiple read replicas and multiple DB instances across different Availability Zones. Users have recently reported errors from the database that indicate that there are too many connections. The company wants to reduce the failover time by 20% when a read replica is promoted to primary writer.
Which solution will meet this requirement?

Options:
A.Switch from Aurora to Amazon RDS with Multi-AZ cluster deployment.
B.Use Amazon RDS Proxy in front of the Aurora database.
C.Switch to Amazon DynamoDB with DynamoDB Accelerator (DAX) for read connections.
D.Switch to Amazon Redshift with relocation capability.

Answer: B

Explanation:

- Correct: RDS Proxy pools/reuses connections and reduces failover impact.

- Option A is wrong because RDS increases failover time.

- Option C is wrong because DynamoDB requires full rearchitecture.

- Option D is wrong because Redshift is for analytics, not transactional workloads.

Question 456:
A company stores text files in Amazon S3. The text files include customer chat messages, date and time information, and customer personally identifiable information (PII). The company needs a solution to provide samples of the conversations to an external service provider for quality control. The external service provider needs to randomly pick sample conversations up to the most recent conversation. The company must not share the customer PII with the external service provider. The solution must scale when the number of customer conversations increases.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an Object Lambda Access Point. Create an AWS Lambda function that redacts the PII when the function reads the file. Instruct the external service provider to access the Object Lambda Access Point.
B.Create a batch process on an Amazon EC2 instance that regularly reads all new files, redacts the PII from the files, and writes the redacted files to a different S3 bucket. Instruct the external service provider to access the bucket that does not contain the PII.
C.Create a web application on an Amazon EC2 instance that presents a list of the files, redacts the PII from the files, and allows the external service provider to download new versions of the files that have the PII redacted.
D.Create an Amazon DynamoDB table. Create an AWS Lambda function that reads only the data in the files that does not contain PII. Configure the Lambda function to store the non-PII data in the DynamoDB table when a new file is written to Amazon S3. Grant the external service provider access to the DynamoDB table.

Answer: A

Explanation:

- Correct: Object Lambda allows dynamic PII redaction at retrieval with low ops.

- Option B is wrong because batch jobs add overhead.

- Option C is wrong because custom web app increases management.

- Option D is wrong because DynamoDB adds unnecessary data pipeline complexity.

Question 457:
A company is running a legacy system on an Amazon EC2 instance. The application code cannot be modified, and the system cannot run on more than one instance. A solutions architect must design a resilient solution that can improve the recovery time for the system. What should the solutions architect recommend to meet these requirements?

Options:
A.Enable termination protection for the EC2 instance.
B.Configure the EC2 instance for Multi-AZ deployment.
C.Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure.
D.Launch the EC2 instance with two Amazon Elastic Block Store (Amazon EBS) volumes that use RAID configurations for storage redundancy.

Answer: C

Explanation:

- Correct: CloudWatch alarm with EC2 recovery restores failed instances quickly.

- Option A is wrong because termination protection prevents deletion, not recovery.

- Option B is wrong because EC2 Multi-AZ does not exist.

- Option D is wrong because RAID only protects storage, not instance availability.

Question 458:
A company wants to deploy its containerized application workloads to a VPC across three Availability Zones. The company needs a solution that is highly available across Availability Zones. The solution must require minimal changes to the application.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS Service Auto Scaling to use target tracking scaling. Set the minimum capacity to 3. Set the task placement strategy type to spread with an Availability Zone attribute.
B.Use Amazon Elastic Kubernetes Service (Amazon EKS) self-managed nodes. Configure Application Auto Scaling to use target tracking scaling. Set the minimum capacity to 3.
C.Use Amazon EC2 Reserved Instances. Launch three EC2 instances in a spread placement group. Configure an Auto Scaling group to use target tracking scaling. Set the minimum capacity to 3.
D.Use an AWS Lambda function. Configure the Lambda function to connect to a VPC. Configure Application Auto Scaling to use Lambda as a scalable target. Set the minimum capacity to 3.

Answer: A

Explanation:

- Correct: ECS with Fargate or managed placement across AZs reduces ops and provides HA.

- Option B is wrong because EKS self-managed nodes add complexity.

- Option C is wrong because Reserved Instances don't autoscale properly.

- Option D is wrong because Lambda isn't suited for containerized workloads.

Question 459:
A media company stores movies in Amazon S3. Each movie is stored in a single video file that ranges from 1 GB to 10 GB in size. The company must be able to provide the streaming content of a movie within 5 minutes of a user purchase. There is higher demand for movies that are less than 20 years old than for movies that are more than 20 years old. The company wants to minimize hosting service costs based on demand.
Which solution will meet these requirements?

Options:
A.Store all media content in Amazon S3. Use S3 Lifecycle policies to move media data into the Infrequent Access tier when the demand for a movie decreases.
B.Store newer movie video files in S3 Standard. Store older movie video files in S3 Standard-Infrequent Access (S3 Standard-IA). When a user orders an older movie, retrieve the video file by using standard retrieval.
C.Store newer movie video files in S3 Intelligent-Tiering. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using expedited retrieval.
D.Store newer movie video files in S3 Standard. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using bulk retrieval.

Answer: C

Explanation:

- Correct: Intelligent-Tiering optimizes newer content cost; Glacier Flexible with expedited retrieval ensures <5 min availability.

- Option A is wrong because IA tier doesn't scale as cost-efficient as Intelligent-Tiering.

- Option B is wrong because retrieval from IA is slower than needed.

- Option D is wrong because bulk retrieval takes hours, not minutes.

Question 460:
A solutions architect needs to design the architecture for an application that a vendor provides as a Docker container image. The container needs 50 GB of storage available for temporary files. The infrastructure must be serverless.
Which solution meets these requirements with the LEAST operational overhead?

Options:
A.Create an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume that has more than 50 GB of space.
B.Create an AWS Lambda function that uses the Docker container image with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space.
C.Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the AWS Fargate launch type. Create a task definition for the container image with an Amazon Elastic File System (Amazon EFS) volume. Create a service with that task definition.
D.Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the Amazon EC2 launch type with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space. Create a task definition for the container image. Create a service with that task definition.

Answer: C

Explanation:

- Correct: ECS with Fargate + EFS provides serverless compute + shared storage.

- Option A is wrong because Lambda ephemeral storage max is 10 GB.

- Option B is wrong because Lambda doesn't integrate with EBS.

- Option D is wrong because EC2 launch type adds infrastructure overhead.

Question 461:
A company needs to use its on-premises LDAP directory service to authenticate its users to the AWS Management Console. The directory service is not compatible with Security Assertion Markup Language (SAML).
Which solution meets these requirements?

Options:
A.Enable AWS IAM Identity Center (AWS Single Sign-On) between AWS and the on-premises LDAP.
B.Create an IAM policy that uses AWS credentials, and integrate the policy into LDAP.
C.Set up a process that rotates the IAM credentials whenever LDAP credentials are updated.
D.Develop an on-premises custom identity broker application or process that uses AWS Security Token Service (AWS STS) to get short-lived credentials.

Answer: D

Explanation:

- Correct: Identity broker allows non-SAML LDAP to issue temporary STS credentials.

- Option A is wrong because IAM Identity Center requires SAML-compatible IdP.

- Option B is wrong because IAM policies don't integrate with LDAP.

- Option C is wrong because rotating IAM creds doesn't authenticate LDAP users.

Question 462:
A company stores multiple Amazon Machine Images (AMIs) in an AWS account to launch its Amazon EC2 instances. The AMIs contain critical data and configurations that are necessary for the company's operations. The company wants to implement a solution that will recover accidentally deleted AMIs quickly and efficiently.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create Amazon Elastic Block Store (Amazon EBS) snapshots of the AMIs. Store the snapshots in a separate AWS account.
B.Copy all AMIs to another AWS account periodically.
C.Create a retention rule in Recycle Bin.
D.Upload the AMIs to an Amazon S3 bucket that has Cross-Region Replication.

Answer: C

Explanation:

- Correct: Recycle Bin protects AMIs from accidental deletion, enabling fast recovery.

- Option A is wrong because snapshots don't guarantee AMI recovery flow.

- Option B is wrong because manual copying adds overhead.

- Option D is wrong because AMIs cannot be stored directly in S3.

Question 463:
A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.
What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

Options:
A.Use AWS Snowmobile to ship the data to AWS.
B.Order multiple AWS Snowball devices to ship the data to AWS.
C.Enable Amazon S3 Transfer Acceleration and securely upload the data.
D.Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Answer: B

Explanation:

- Correct: Snowball is ideal for 150 TB migrations, faster than network-based uploads.

- Option A is wrong because Snowmobile is for petabytes/exabytes, not 150 TB.

- Option C is wrong because S3TA over 100 Mbps is too slow for deadline.

- Option D is wrong because VPN doesn't increase bandwidth.

Question 464:
A company wants to migrate its three-tier application from on premises to AWS. The web tier and the application tier are running on third-party virtual machines (VMs). The database tier is running on MySQL. The company needs to migrate the application by making the fewest possible changes to the architecture. The company also needs a database solution that can restore data to a specific point in time.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Migrate the web tier and the application tier to Amazon EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.
B.Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon Aurora MySQL in private subnets.
C.Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.
D.Migrate the web tier and the application tier to Amazon EC2 instances in public subnets. Migrate the database tier to Amazon Aurora MySQL in public subnets.

Answer: A

Explanation:

- Correct: EC2 mimics existing VM tiers, RDS MySQL supports PITR with low ops.

- Option B is wrong because Aurora requires more changes.

- Option C is wrong because placing web tier in public subnet adds security risks.

- Option D is wrong because DB should not be public.

Question 465:
A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.
How should a solutions architect provide access to the SQS queue?

Options:
A.Create an instance profile that provides the other company access to the SQS queue.
B.Create an IAM policy that provides the other company access to the SQS queue.
C.Create an SQS access policy that provides the other company access to the SQS queue.
D.Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Answer: C

Explanation:

- Correct: SQS supports resource-based access policies for cross-account access.

- Option A is wrong because instance profiles are for EC2 roles.

- Option B is wrong because IAM policy in one account cannot directly grant another account access.

- Option D is wrong because SNS policies are irrelevant to SQS access.

Question 466:
A company's developers want a secure way to gain SSH access on the company's Amazon EC2 instances that run the latest version of Amazon Linux. The developers work remotely and in the corporate office. The company wants to use AWS services as a part of the solution. The EC2 instances are hosted in a VPC private subnet and access the internet through a NAT gateway that is deployed in a public subnet.
What should a solutions architect do to meet these requirements MOST cost-effectively?

Options:
A.Create a bastion host in the same subnet as the EC2 instances. Grant the ec2:CreateVpnConnection IAM permission to the developers. Install EC2 Instance Connect so that the developers can connect to the EC2 instances.
B.Create an AWS Site-to-Site VPN connection between the corporate network and the VPC. Instruct the developers to use the Site-to-Site VPN connection to access the EC2 instances when the developers are on the corporate network. Instruct the developers to set up another VPN connection for access when they work remotely.
C.Create a bastion host in the public subnet of the VPC. Configure the security groups and SSH keys of the bastion host to only allow connections and SSH authentication from the developers' corporate and remote networks. Instruct the developers to connect through the bastion host by using SSH to reach the EC2 instances.
D.Attach the AmazonSSMManagedInstanceCore IAM policy to an IAM role that is associated with the EC2 instances. Instruct the developers to use AWS Systems Manager Session Manager to access the EC2 instances.

Answer: D

Explanation:

- Correct: SSM Session Manager provides secure, auditable, and keyless SSH-like access.

- Option A is wrong because bastion in private subnet won't work.

- Option B is wrong because dual VPN setup is costly/complex.

- Option C is wrong because bastion adds management overhead.

Question 467:
A pharmaceutical company is developing a new drug. The volume of data that the company generates has grown exponentially over the past few months. The company's researchers regularly require a subset of the entire dataset to be immediately available with minimal lag. However, the entire dataset does not need to be accessed on a daily basis. All the data currently resides in on-premises storage arrays, and the company wants to reduce ongoing capital expenses.
Which storage solution should a solutions architect recommend to meet these requirements?

Options:
A.Run AWS DataSync as a scheduled cron job to migrate the data to an Amazon S3 bucket on an ongoing basis.
B.Deploy an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.
C.Deploy an AWS Storage Gateway volume gateway with cached volumes with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.
D.Configure an AWS Site-to-Site VPN connection from the on-premises environment to AWS. Migrate data to an Amazon Elastic File System (Amazon EFS) file system.

Answer: C

Explanation:

- Correct: Volume Gateway with cached volumes keeps subset of hot data locally, rest in S3.

- Option A is wrong because DataSync migration won't maintain subset access.

- Option B is wrong because file gateway is for SMB/NFS, not volume storage access.

- Option D is wrong because VPN + EFS does not reduce storage capex effectively.

Question 468:
A company has a business-critical application that runs on Amazon EC2 instances. The application stores data in an Amazon DynamoDB table. The company must be able to revert the table to any point within the last 24 hours.
Which solution meets these requirements with the LEAST operational overhead?

Options:
A.Configure point-in-time recovery for the table.
B.Use AWS Backup for the table.
C.Use an AWS Lambda function to make an on-demand backup of the table every hour.
D.Turn on streams on the table to capture a log of all changes to the table in the last 24 hours. Store a copy of the stream in an Amazon S3 bucket.

Answer: A

Explanation:

- Correct: DynamoDB point-in-time recovery (PITR) provides built-in continuous backup within last 35 days.

- Option B is wrong because AWS Backup adds unnecessary overhead.

- Option C is wrong because Lambda backup scheduling adds ops overhead.

- Option D is wrong because streams are not a restore mechanism.

Question 469:
A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.
What should the solutions architect recommend?

Options:
A.Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
B.Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
C.Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
D.Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Answer: B

Explanation:

- Correct: S3 event notifications + Lambda is serverless and cost-efficient.

- Option A is wrong because CloudTrail/AppSync is unrelated.

- Option C is wrong because Kinesis is overkill for S3 file ingestion.

- Option D is wrong because SNS adds unnecessary layer.

Question 470:
A company's application is deployed on Amazon EC2 instances and uses AWS Lambda functions for an event-driven architecture. The company uses nonproduction development environments in a different AWS account to test new features before the company deploys the features to production. The production instances show constant usage because of customers in different time zones. The company uses nonproduction instances only during business hours on weekdays. The company does not use the nonproduction instances on the weekends. The company wants to optimize the costs to run its application on AWS.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Use On-Demand Instances for the production instances. Use Dedicated Hosts for the nonproduction instances on weekends only.
B.Use Reserved Instances for the production instances and the nonproduction instances. Shut down the nonproduction instances when not in use.
C.Use Compute Savings Plans for the production instances. Use On-Demand Instances for the nonproduction instances. Shut down the nonproduction instances when not in use.
D.Use Dedicated Hosts for the production instances. Use EC2 Instance Savings Plans for the nonproduction instances.

Answer: C

Explanation:

- Correct: Compute Savings Plans cover steady production workloads; On-Demand + scheduling suits dev workloads.

- Option A is wrong because Dedicated Hosts for dev is wasteful.

- Option B is wrong because RIs for dev waste cost during downtime.

- Option D is wrong because Dedicated Hosts are unnecessary.

Question 471:

A company stores data in an on-premises Oracle relational database. The company needs to make the data available in Amazon Aurora PostgreSQL for analysis. The company uses an AWS Site-to-Site VPN connection to connect its on-premises network to AWS. The company must capture the changes that occur to the source database during the migration to Aurora PostgreSQL.

Which solution will meet these requirements?

Options:

A.Use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema. Use the AWS Database Migration Service (AWS DMS) full-load migration task to migrate the data.

B.Use AWS DataSync to migrate the data to an Amazon S3 bucket. Import the S3 data to Aurora PostgreSQL by using the Aurora PostgreSQL aws_s3 extension.

C.Use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema. Use AWS Database Migration Service (AWS DMS) to migrate the existing data and replicate the ongoing changes.

D.Use an AWS Snowball device to migrate the data to an Amazon S3 bucket. Import the S3 data to Aurora PostgreSQL by using the Aurora PostgreSQL aws_s3 extension.

Answer: C

Explanation:

- Correct: SCT converts schema, DMS supports full-load + CDC replication.

- Option A is wrong because it doesn't capture ongoing changes.

- Option B is wrong because DataSync only copies files, not DB changes.

- Option D is wrong because Snowball is for bulk one-time migration.

Question 472:
A company built an application with Docker containers and needs to run the application in the AWS Cloud. The company wants to use a managed service to host the application. The solution must scale in and out appropriately according to demand on the individual container services. The solution also must not result in additional operational overhead or infrastructure to manage.
Which solutions will meet these requirements? (Choose two.)

Options:
A.Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
B.Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate.
C.Provision an Amazon API Gateway API. Connect the API to AWS Lambda to run the containers.
D.Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes.
E.Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes.

Answer: AB

Explanation:

- Correct: ECS + Fargate and EKS + Fargate both eliminate server management and scale per container.

- Option C is wrong because Lambda doesn't run arbitrary Docker containers persistently.

- Option D is wrong because ECS with EC2 adds node management.

- Option E is wrong because EKS with EC2 adds node management.

Question 473:
An ecommerce company is running a seasonal online sale. The company hosts its website on Amazon EC2 instances spanning multiple Availability Zones. The company wants its website to manage sudden traffic increases during the sale.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create an Auto Scaling group that is large enough to handle peak traffic load. Stop half of the Amazon EC2 instances. Configure the Auto Scaling group to use the stopped instances to scale out when traffic increases.
B.Create an Auto Scaling group for the website. Set the minimum size of the Auto Scaling group so that it can handle high traffic volumes without the need to scale out.
C.Use Amazon CloudFront and Amazon ElastiCache to cache dynamic content with an Auto Scaling group set as the origin. Configure the Auto Scaling group with the instances necessary to populate CloudFront and ElastiCache. Scale in after the cache is fully populated.
D.Configure an Auto Scaling group to scale out as traffic increases. Create a launch template to start new instances from a preconfigured Amazon Machine Image (AMI).

Answer: D

Explanation:

- Correct: Auto Scaling with launch templates ensures cost efficiency and elasticity.

- Option A is wrong because managing stopped instances is inefficient.

- Option B is wrong because pre-provisioning all peak capacity wastes cost.

- ~~Option C is wrong because CloudFront/ElastiCache won't eliminate need for scaling.~~

Question 474:
A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.
What should the solutions architect do to meet these requirements with the LEAST operational overhead?

Options:
A.Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.
B.Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
C.Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.
D.Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

Answer: B

Explanation:

- Correct: AWS Config managed rule automatically detects SSH open to world + alerts.

- Option A is wrong because custom Lambda adds management.

- Option C is wrong because IAM role won't detect compliance violations.

- Option D is wrong because SCPs restrict actions, but don't alert.

Question 475:
A company has deployed an application in an AWS account. The application consists of microservices that run on AWS Lambda and Amazon Elastic Kubernetes Service (Amazon EKS). A separate team supports each microservice. The company has multiple AWS accounts and wants to give each team its own account for its microservices. A solutions architect needs to design a solution that will provide service-to-service communication over HTTPS (port 443). The solution also must provide a service registry for service discovery.
Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A.Create an inspection VPC. Deploy an AWS Network Firewall firewall to the inspection VPC. Attach the inspection VPC to a new transit gateway. Route VPC-to-VPC traffic to the inspection VPC. Apply firewall rules to allow only HTTPS communication.
B.Create a VPC Lattice service network. Associate the microservices with the service network. Define HTTPS listeners for each service. Register microservice compute resources as targets. Identify VPCs that need to communicate with the services. Associate those VPCs with the service network.
C.Create a Network Load Balancer (NLB) with an HTTPS listener and target groups for each microservice. Create an AWS PrivateLink endpoint service for each microservice. Create an interface VPC endpoint in each VPC that needs to consume that microservice.
D.Create peering connections between VPCs that contain microservices. Create a prefix list for each service that requires a connection to a client. Create route tables to route traffic to the appropriate VPC. Create security groups to allow only HTTPS communication.

Answer: B

Explanation:

- Correct: VPC Lattice simplifies multi-account, multi-service HTTPS comms + service registry.

- Option A is wrong because firewall adds complexity.

- Option C is wrong because PrivateLink is for one-to-one service publishing, not registry.

- Option D is wrong because VPC peering doesn't scale well for multiple services.

Question 476:
A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity, developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots, replication, and sub-millisecond response times.
What should the solutions architect recommend to solve these issues?

Options:
A.Migrate the database to Amazon Aurora with Aurora Replicas.
B.Migrate the database to Amazon DynamoDB with global tables.
C.Add an Amazon ElastiCache for Redis layer in front of the database.
D.Add an Amazon ElastiCache for Memcached layer in front of the database.

Answer: C

Explanation:

- Correct: Redis provides sub-ms latency, caching, replication, snapshots, and improves read performance.

- Option A is wrong because Aurora replicas still have latency and higher cost.

- Option B is wrong because DynamoDB requires re-architecture.

- Option D is wrong because Memcached lacks persistence and replication.

Question 477:
A company uses AWS Organizations for its multi-account AWS setup. The security organizational unit (OU) of the company needs to share approved Amazon Machine Images (AMIs) with the development OU. The AMIs are created by using AWS Key Management Service (AWS KMS) encrypted snapshots.
Which solution will meet these requirements? (Choose two.)

Options:
A.Add the development team's OU Amazon Resource Name (ARN) to the launch permission list for the AMIs.
B.Add the Organizations root Amazon Resource Name (ARN) to the launch permission list for the AMIs.
C.Update the key policy to allow the development team's OU to use the AWS KMS keys that are used to decrypt the snapshots.
D.Add the development team's account Amazon Resource Name (ARN) to the launch permission list for the AMIs.
E.Recreate the AWS KMS key. Add a key policy to allow the Organizations root Amazon Resource Name (ARN) to use the AWS KMS key.

Answer: AC

Explanation:

- Correct: Must share AMI launch permissions and grant KMS key access to decrypt snapshots.

- Option B is wrong because sharing with Organizations root ARN doesn't directly grant OU usage.

- Option D is wrong because sharing needs KMS permissions too.

- Option E is wrong because recreating the key is unnecessary.

Question 478:
A data analytics company has 80 offices that are distributed globally. Each office hosts 1 PB of data and has between 1 and 2 Gbps of internet bandwidth. The company needs to perform a one-time migration of a large amount of data from its offices to Amazon S3. The company must complete the migration within 4 weeks.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Establish a new 10 Gbps AWS Direct Connect connection to each office. Transfer the data to Amazon S3.
B.Use multiple AWS Snowball Edge storage-optimized devices to store and transfer the data to Amazon S3.
C.Use an AWS Snowmobile to store and transfer the data to Amazon S3.
D.Set up an AWS Storage Gateway Volume Gateway to transfer the data to Amazon S3.

Answer: B

Explanation:

- Correct: Snowball Edge supports PB-scale migration, cheaper than Direct Connect for one-time.

- Option A is wrong because DX setup takes months, not 4 weeks.

- Option C is wrong because Snowmobile is for exabytes, not 80 PB.

- Option D is wrong because Storage Gateway is for hybrid ongoing use.

Question 479:
A company has an Amazon Elastic File System (Amazon EFS) file system that contains a reference dataset. The company has applications on Amazon EC2 instances that need to read the dataset. However, the applications must not be able to change the dataset. The company wants to use IAM access control to prevent the applications from being able to modify or delete the dataset.
Which solution will meet these requirements?

Options:
A.Mount the EFS file system in read-only mode from within the EC2 instances.
B.Create a resource policy for the EFS file system that denies the elasticfilesystem:ClientWrite action to the IAM roles that are attached to the EC2 instances.
C.Create an identity policy for the EFS file system that denies the elasticfilesystem:ClientWrite action on the EFS file system.
D.Create an EFS access point for each application. Use Portable Operating System Interface (POSIX) file permissions to allow read-only access to files in the root directory.

Answer: B

Explanation:

- Correct: Resource policy directly blocks write actions regardless of mount settings.

- Option A is wrong because mount options can be bypassed.

- Option C is wrong because IAM identity policies can't enforce write denial at file system level.

- Option D is wrong because POSIX permissions don't provide IAM-based enforcement.

Question 480:
A company has hired an external vendor to perform work in the company's AWS account. The vendor uses an automated tool that is hosted in an AWS account that the vendor owns. The vendor does not have IAM access to the company's AWS account. The company needs to grant the vendor access to the company's AWS account.
Which solution will meet these requirements MOST securely?

Options:
A.Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
B.Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
C.Create an IAM group in the company's account. Add the automated tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
D.Create an IAM user in the company's account that has a permission boundary that allows the vendor's account. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.

Answer: A

Explanation:

- Correct: Cross-account IAM role with trust policy is secure and least privilege.

- Option B is wrong because IAM user credentials are less secure.

- Option C is wrong because IAM group cannot include external users.

Question 481:
A company wants to run its experimental workloads in the AWS Cloud. The company has a budget for cloud spending. The company's CFO is concerned about cloud spending accountability for each department. The CFO wants to receive notification when the spending threshold reaches 60% of the budget.
Which solution will meet these requirements?

Options:
A.Use cost allocation tags on AWS resources to label owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.
B.Use AWS Cost Explorer forecasts to determine resource owners. Use AWS Cost Anomaly Detection to create alert threshold notifications when spending exceeds 60% of the budget.
C.Use cost allocation tags on AWS resources to label owners. Use AWS Support API on AWS Trusted Advisor to create alert threshold notifications when spending exceeds 60% of the budget.
D.Use AWS Cost Explorer forecasts to determine resource owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.

Answer: A

Explanation:

- Correct: Tags + AWS Budgets provide accountability + alerts.

- Option B is wrong because Cost Anomaly Detection is not budget-based.

- Option C is wrong because Trusted Advisor is not for budget alerts.

- Option D is wrong because Cost Explorer forecasts don't provide direct alerts.

Question 482:
A company wants to deploy an internal web application on AWS. The web application must be accessible only from the company's office. The company needs to download security patches for the web application from the internet. The company has created a VPC and has configured an AWS Site-to-Site VPN connection to the company's office. A solutions architect must design a secure architecture for the web application.
Which solution will meet these requirements?

Options:
A.Deploy the web application on Amazon EC2 instances in public subnets behind a public Application Load Balancer (ALB). Attach an internet gateway to the VPC. Set the inbound source of the ALB's security group to 0.0.0.0/0.
B.Deploy the web application on Amazon EC2 instances in private subnets behind an internal Application Load Balancer (ALB). Deploy NAT gateways in public subnets. Attach an internet gateway to the VPC. Set the inbound source of the ALB's security group to the company's office network CIDR block.
C.Deploy the web application on Amazon EC2 instances in public subnets behind an internal Application Load Balancer (ALB). Deploy NAT gateways in private subnets. Attach an internet gateway to the VPC. Set the outbound destination of the ALB's security group to the company's office network CIDR block.
D.Deploy the web application on Amazon EC2 instances in private subnets behind a public Application Load Balancer (ALB). Attach an internet gateway to the VPC. Set the outbound destination of the ALB's security group to 0.0.0.0/0.

Answer: B

Explanation:

- Correct: Private subnets + internal ALB restrict access, NAT for patches.

- Option A is wrong because 0.0.0.0/0 exposes app publicly.

- Option C is wrong because wrong subnet usage.

- Option D is wrong because public ALB exposes app.

Question 483:
A company maintains its accounting records in a custom application that runs on Amazon EC2 instances. The company needs to migrate the data to an AWS managed service for development and maintenance of the application data. The solution must require minimal operational support and provide immutable, cryptographically verifiable logs of data changes. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Copy the records from the application into an Amazon Redshift cluster.
B.Copy the records from the application into an Amazon Neptune cluster.
C.Copy the records from the application into an Amazon Timestream database.
D.Copy the records from the application into an Amazon Quantum Ledger Database (Amazon QLDB) ledger.

Answer: D

Explanation:

- Correct: QLDB provides immutable, cryptographically verifiable transaction logs.

- Option A is wrong because Redshift is for analytics.

- Option B is wrong because Neptune is for graphs.

- Option C is wrong because Timestream is for time series.

Question 484:
A company's marketing data is uploaded from multiple sources to an Amazon S3 bucket. A series of data preparation jobs aggregate the data for reporting. The data preparation jobs need to run at regular intervals in parallel. A few jobs need to run in a specific order later. The company wants to remove the operational overhead of job error handling, retry logic, and state management.
Which solution will meet these requirements?

Options:
A.Use an AWS Lambda function to process the data as soon as the data is uploaded to the S3 bucket. Invoke other Lambda functions at regularly scheduled intervals.
B.Use Amazon Athena to process the data. Use Amazon EventBridge Scheduler to invoke Athena on a regular interval.
C.Use AWS Glue DataBrew to process the data. Use an AWS Step Functions state machine to run the DataBrew data preparation jobs.
D.Use AWS Data Pipeline to process the data. Schedule Data Pipeline to process the data once at midnight.

Answer: C

Explanation:

- Correct: Glue DataBrew + Step Functions handle orchestration, retries, error handling.

- Option A is wrong because it lacks workflow management.

- Option B is wrong because Athena is not for preparation workflows.

- Option D is wrong because Data Pipeline is outdated.

Question 485:
A solutions architect is designing a payment processing application that runs on AWS Lambda in private subnets across multiple Availability Zones. The application uses multiple Lambda functions and processes millions of transactions each day. The architecture must ensure that the application does not process duplicate payments.
Which solution will meet these requirements?

Options:
A.Use Lambda to retrieve all due payments. Publish the due payments to an Amazon S3 bucket. Configure the S3 bucket with an event notification to invoke another Lambda function to process the due payments.
B.Use Lambda to retrieve all due payments. Publish the due payments to an Amazon Simple Queue Service (Amazon SQS) queue. Configure another Lambda function to poll the SQS queue and to process the due payments.
C.Use Lambda to retrieve all due payments. Publish the due payments to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Configure another Lambda function to poll the FIFO queue and to process the due payments.
D.Use Lambda to retrieve all due payments. Store the due payments in an Amazon DynamoDB table. Configure streams on the DynamoDB table to invoke another Lambda function to process the due payments.

Answer: C

Explanation:

- Correct: SQS FIFO ensures exactly-once processing, preventing duplicates.

- Option A is wrong because S3 event notifications don't prevent duplicates.

- Option B is wrong because standard SQS doesn't guarantee exactly-once.

- Option D is wrong because DynamoDB streams don't prevent duplicates.

Question 486:

A company runs multiple workloads in its on-premises data center. The company's data center cannot scale fast enough to meet the company's expanding business needs. The company wants to collect usage and configuration data about the on-premises servers and workloads to plan a migration to AWS.

Which solution will meet these requirements?

Options:

A.Set the home AWS Region in AWS Migration Hub. Use AWS Systems Manager to collect data about the on-premises servers.

B.Set the home AWS Region in AWS Migration Hub. Use AWS Application Discovery Service to collect data about the on-premises servers.

C.Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates. Use AWS Trusted Advisor to collect data about the on-premises servers.

D.Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates. Use AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers.

Answer: B

Explanation:

- Correct: Migration Hub + Application Discovery Service collects on-premises server data.

- Option A is wrong because SSM requires hybrid activation but doesn't provide full discovery.

- Option C is wrong because Trusted Advisor doesn't analyze on-prem infra.

- Option D is wrong because DMS is for DB migration, not infra discovery.

Question 487:

A company has an organization in AWS Organizations that has all features enabled. The company requires that all API calls and logins in any existing or new AWS account must be audited. The company needs a managed solution to prevent additional work and to minimize costs. The company also needs to know when any AWS account is not compliant with the AWS Foundational Security Best Practices (FSBP) standard.

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

Options:

A.Deploy an AWS Control Tower environment in the Organizations management account. Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.

B.Deploy an AWS Control Tower environment in a dedicated Organizations member account. Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.

C.Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ). Submit an RFC to self-service provision Amazon GuardDuty in the MALZ.

D.Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ). Submit an RFC to self-service provision AWS Security Hub in the MALZ.

Answer: A

Explanation:

- Correct: Control Tower with Security Hub in management account automates compliance + auditing.

- Option B is wrong because Control Tower must be in management account.

- Option C is wrong because GuardDuty doesn't check FSBP compliance.

- Option D is wrong because AMS adds unnecessary overhead.

Question 488:
A company has stored 10 TB of log files in Apache Parquet format in an Amazon S3 bucket. The company occasionally needs to use SQL to analyze the log files.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create an Amazon Aurora MySQL database. Migrate the data from the S3 bucket into Aurora by using AWS Database Migration Service (AWS DMS). Issue SQL statements to the Aurora database.
B.Create an Amazon Redshift cluster. Use Redshift Spectrum to run SQL statements directly on the data in the S3 bucket.
C.Create an AWS Glue crawler to store and retrieve table metadata from the S3 bucket. Use Amazon Athena to run SQL statements directly on the data in the S3 bucket.
D.Create an Amazon EMR cluster. Use Apache Spark SQL to run SQL statements directly on the data in the S3 bucket.

Answer: C

Explanation:

- Correct: Glue crawler + Athena provides serverless, pay-per-query SQL.

- Option A is wrong because Aurora migration is expensive.

- Option B is wrong because Redshift adds cost for occasional queries.

- Option D is wrong because EMR cluster adds ops overhead.

Question 489:
A company needs a solution to prevent AWS CloudFormation stacks from deploying AWS Identity and Access Management (IAM) resources that include an inline policy or "*" in the statement. The solution must also prohibit deployment of Amazon EC2 instances with public IP addresses. The company has AWS Control Tower enabled in its organization in AWS Organizations.
Which solution will meet these requirements?

Options:
A.Use AWS Control Tower proactive controls to block deployment of EC2 instances with public IP addresses and inline policies with elevated access or " ".
B.Use AWS Control Tower detective controls to block deployment of EC2 instances with public IP addresses and inline policies with elevated access or "*".
C.Use AWS Config to create rules for EC2 and IAM compliance. Configure the rules to run an AWS Systems Manager Session Manager automation to delete a resource when it is not compliant.
D.Use a service control policy (SCP) to block actions for the EC2 instances and IAM resources if the actions lead to noncompliance.

Answer: D

Explanation:

- Correct: SCPs enforce org-level restrictions to block specific actions.

- Option A is wrong because proactive controls are limited.

- Option B is wrong because detective controls only detect, not prevent.

- Option C is wrong because Config detects/remediates, not blocks at creation.

Question 490:
A company's web application that is hosted in the AWS Cloud recently increased in popularity. The web application currently exists on a single Amazon EC2 instance in a single public subnet. The web application has not been able to meet the demand of the increased web traffic. The company needs a solution that will provide high availability and scalability to meet the increased user demand without rewriting the web application.
Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Replace the EC2 instance with a larger compute optimized instance.
B.Configure Amazon EC2 Auto Scaling with multiple Availability Zones in private subnets.
C.Configure a NAT gateway in a public subnet to handle web requests.
D.Replace the EC2 instance with a larger memory optimized instance.
E.Configure an Application Load Balancer in a public subnet to distribute web traffic.

Answer: BE

Explanation:

- Correct: Auto Scaling + ALB provides HA + scalability.

- Option A is wrong because scaling vertically won't ensure HA.

- Option C is wrong because NAT is not for inbound traffic.

- Option D is wrong because memory optimization doesn't solve scaling.

Question 491:
A company has AWS Lambda functions that use environment variables. The company does not want its developers to see environment variables in plaintext.
Which solution will meet these requirements?

Options:
A.Deploy code to Amazon EC2 instances instead of using Lambda functions.
B.Configure SSL encryption on the Lambda functions to use AWS CloudHSM to store and encrypt the environment variables.
C.Create a certificate in AWS Certificate Manager (ACM). Configure the Lambda functions to use the certificate to encrypt the environment variables.
D.Create an AWS Key Management Service (AWS KMS) key. Enable encryption helpers on the Lambda functions to use the KMS key to store and encrypt the environment variables.

Answer: D

Explanation:

- Correct: Lambda encryption helpers + KMS protect env vars.

- Option A is wrong because moving to EC2 doesn't solve problem.

- Option B is wrong because CloudHSM adds complexity.

- Option C is wrong because ACM is for SSL/TLS, not env vars.

Question 492:
An analytics company uses Amazon VPC to run its multi-tier services. The company wants to use RESTful APIs to offer a web analytics service to millions of users. Users must be verified by using an authentication service to access the APIs.
Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Configure an Amazon Cognito user pool for user authentication. Implement Amazon API Gateway REST APIs with a Cognito authorizer.
B.Configure an Amazon Cognito identity pool for user authentication. Implement Amazon API Gateway HTTP APIs with a Cognito authorizer.
C.Configure an AWS Lambda function to handle user authentication. Implement Amazon API Gateway REST APIs with a Lambda authorizer.
D.Configure an IAM user to handle user authentication. Implement Amazon API Gateway HTTP APIs with an IAM authorizer.

Answer: A

Explanation:

- Correct: Cognito user pool + API Gateway REST APIs is standard for scalable user auth.

- Option B is wrong because identity pools are for AWS resource access, not API auth.

- Option C is wrong because custom Lambda authorizer adds ops overhead.

- Option D is wrong because IAM users are not scalable for millions of users.

Question 493:
A company has a mobile app for customers. The app's data is sensitive and must be encrypted at rest. The company uses AWS Key Management Service (AWS KMS). The company needs a solution that prevents the accidental deletion of KMS keys. The solution must use Amazon Simple Notification Service (Amazon SNS) to send an email notification to administrators when a user attempts to delete a KMS key.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create an Amazon EventBridge rule that reacts when a user tries to delete a KMS key. Configure an AWS Config rule that cancels any deletion of a KMS key. Add the AWS Config rule as a target of the EventBridge rule. Create an SNS topic that notifies the administrators.
B.Create an AWS Lambda function that has custom logic to prevent KMS key deletion. Create an Amazon CloudWatch alarm that is activated when a user tries to delete a KMS key. Create an Amazon EventBridge rule that invokes the Lambda function when the DeleteKey operation is performed. Create an SNS topic. Configure the EventBridge rule to publish an SNS message that notifies the administrators.
C.Create an Amazon EventBridge rule that reacts when the KMS DeleteKey operation is performed. Configure the rule to initiate an AWS Systems Manager Automation runbook. Configure the runbook to cancel the deletion of the KMS key. Create an SNS topic. Configure the EventBridge rule to publish an SNS message that notifies the administrators.
D.Create an AWS CloudTrail trail. Configure the trail to deliver logs to a new Amazon CloudWatch log group. Create a CloudWatch alarm based on the metric filter for the CloudWatch log group. Configure the alarm to use Amazon SNS to notify the administrators when the KMS DeleteKey operation is performed.

Answer: C

Explanation:

- Correct: EventBridge + SSM Automation cancels deletion and alerts via SNS.

- Option A is wrong because Config doesn't prevent deletion in real time.

- Option B is wrong because custom Lambda adds complexity.

- Option D is wrong because CloudTrail + CloudWatch only notifies, doesn't block.

Question 494:
A company wants to analyze and generate reports to track the usage of its mobile app. The app is popular and has a global user base. The company uses a custom report building program to analyze application usage. The program generates multiple reports during the last week of each month. The program takes less than 10 minutes to produce each report. The company rarely uses the program to generate reports outside of the last week of each month The company wants to generate reports in the least amount of time when the reports are requested.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Run the program by using Amazon EC2 On-Demand Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.
B.Run the program in AWS Lambda. Create an Amazon EventBridge rule to run a Lambda function when reports are requested.
C.Run the program in Amazon Elastic Container Service (Amazon ECS). Schedule Amazon ECS to run the program when reports are requested.
D.Run the program by using Amazon EC2 Spot Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.

Answer: B

Explanation:

- Correct: Lambda is serverless, cost-efficient, quick for <15 min jobs.

- Option A is wrong because EC2 on-demand is costly when idle.

- Option C is wrong because ECS requires more setup.

- Option D is wrong because Spot may terminate and not needed.

Question 495:
A company is designing a tightly coupled high performance computing (HPC) environment in the AWS Cloud. The company needs to include features that will optimize the HPC environment for networking and storage.
Which combination of solutions will meet these requirements? (Choose two.)

Options:
A.Create an accelerator in AWS Global Accelerator. Configure custom routing for the accelerator.
B.Create an Amazon FSx for Lustre file system. Configure the file system with scratch storage.
C.Create an Amazon CloudFront distribution. Configure the viewer protocol policy to be HTTP and HTTPS.
D.Launch Amazon EC2 instances. Attach an Elastic Fabric Adapter (EFA) to the instances.
E.Create an AWS Elastic Beanstalk deployment to manage the environment.

Answer: BD

Explanation:

- Correct: FSx for Lustre + EFA are designed for HPC workloads.

- Option A is wrong because Global Accelerator is for edge routing.

- Option C is wrong because CloudFront is for CDN, not HPC.

- Option E is wrong because Beanstalk is not used for HPC.

Question 496:
A company needs a solution to prevent photos with unwanted content from being uploaded to the company's web application. The solution must not involve training a machine learning (ML) model.
Which solution will meet these requirements?

Options:
A.Create and deploy a model by using Amazon SageMaker Autopilot. Create a real-time endpoint that the web application invokes when new photos are uploaded.
B.Create an AWS Lambda function that uses Amazon Rekognition to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.
C.Create an Amazon CloudFront function that uses Amazon Comprehend to detect unwanted content. Associate the function with the web application.
D.Create an AWS Lambda function that uses Amazon Rekognition Video to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.

Answer: B

Explanation:

- Correct: Rekognition supports image moderation directly without training.

- Option A is wrong because SageMaker requires training.

- Option C is wrong because Comprehend is for text.

- Option D is wrong because Rekognition Video is for streaming video, not still photos.

Question 497:
A company uses AWS to run its ecommerce platform. The platform is critical to the company's operations and has a high volume of traffic and transactions. The company configures a multi-factor authentication (MFA) device to secure its AWS account root user credentials. The company wants to ensure that it will not lose access to the root user account if the MFA device is lost.
Which solution will meet these requirements?

Options:
A.Set up a backup administrator account that the company can use to log in if the company loses the MFA device.
B.Add multiple MFA devices for the root user account to handle the disaster scenario.
C.Create a new administrator account when the company cannot access the root account.
D.Attach the administrator policy to another IAM user when the company cannot access the root account.

Answer: B

Explanation:

- Correct: Root user supports multiple MFA devices for redundancy.

- Option A is wrong because backup admin account does not replace root.

- Option C is wrong because new account creation won't recover lost access.

- Option D is wrong because IAM users can't replace root access.

Question 498:
A social media company is creating a rewards program website for its users. The company gives users points when users create and upload videos to the website. Users redeem their points for gifts or discounts from the company's affiliated partners. A unique ID identifies users. The partners refer to this ID to verify user eligibility for rewards. The partners want to receive notification of user IDs through an HTTP endpoint when the company gives users points. Hundreds of vendors are interested in becoming affiliated partners every day. The company wants to design an architecture that gives the website the ability to add partners rapidly in a scalable way.
Which solution will meet these requirements with the LEAST implementation effort?

Options:
A.Create an Amazon Timestream database to keep a list of affiliated partners. Implement an AWS Lambda function to read the list. Configure the Lambda function to send user IDs to each partner when the company gives users points.
B.Create an Amazon Simple Notification Service (Amazon SNS) topic. Choose an endpoint protocol. Subscribe the partners to the topic. Publish user IDs to the topic when the company gives users points.
C.Create an AWS Step Functions state machine. Create a task for every affiliated partner. Invoke the state machine with user IDs as input when the company gives users points.
D.Create a data stream in Amazon Kinesis Data Streams. Implement producer and consumer applications. Store a list of affiliated partners in the data stream. Send user IDs when the company gives users points.

Answer: B

Explanation:

- Correct: SNS supports HTTP subscriptions, scalable to many vendors.

- Option A is wrong because Timestream is time-series DB, not messaging.

- Option C is wrong because Step Functions is not designed for dynamic partner scaling.

- Option D is wrong because Kinesis requires consumer apps, adds complexity.

Question 499:

A company needs to extract the names of ingredients from recipe records that are stored as text files in an Amazon S3 bucket. A web application will use the ingredient names to query an Amazon DynamoDB table and determine a nutrition score. The application can handle non-food records and errors. The company does not have any employees who have machine learning knowledge to develop this solution.

Which solution will meet these requirements MOST cost-effectively?

Options:

A.Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur. Program the Lambda function to analyze the object and extract the ingredient names by using Amazon Comprehend. Store the Amazon Comprehend output in the DynamoDB table.

B.Use an Amazon EventBridge rule to invoke an AWS Lambda function when PutObject requests occur. Program the Lambda function to analyze the object by using Amazon Forecast to extract the ingredient names. Store the Forecast output in the DynamoDB table.

C.Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur. Use Amazon Polly to create audio recordings of the recipe records. Save the audio files in the S3 bucket. Use Amazon SNS to send a URL as a message to employees. Instruct the employees to listen to the audio files and calculate the nutrition score. Store the ingredient names in the DynamoDB table.

D.Use an Amazon EventBridge rule to invoke an AWS Lambda function when a PutObject request occurs. Program the Lambda function to analyze the object and extract the ingredient names by using Amazon SageMaker. Store the inference output from the SageMaker endpoint in the DynamoDB table.

Answer: A

Explanation:

- Correct: Comprehend NLP can extract entities without ML expertise.

- Option B is wrong because Forecast is for time-series forecasting.

- Option C is wrong because Polly/audio/manual process is inefficient.

- Option D is wrong because SageMaker requires ML expertise.

Question 500:
A company needs to create an AWS Lambda function that will run in a VPC in the company's primary AWS account. The Lambda function needs to access files that the company stores in an Amazon Elastic File System (Amazon EFS) file system. The EFS file system is located in a secondary AWS account. As the company adds files to the file system, the solution must scale to meet the demand.
Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create a new EFS file system in the primary account. Use AWS DataSync to copy the contents of the original EFS file system to the new EFS file system.
B.Create a VPC peering connection between the VPCs that are in the primary account and the secondary account.
C.Create a second Lambda function in the secondary account that has a mount that is configured for the file system. Use the primary account's Lambda function to invoke the secondary account's Lambda function.
D.Move the contents of the file system to a Lambda layer. Configure the Lambda layer's permissions to allow the company's secondary account to use the Lambda layer.

Answer: B

Explanation:

- Correct: VPC peering enables cross-account VPC-level EFS access with minimal cost.

- Option A is wrong because duplicating data increases cost.

- Option C is wrong because two-step Lambda invocation adds complexity.

- Option D is wrong because Lambda layers are not designed for large dynamic file storage

Question 501:
A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection. The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity. Which solution meets these requirements?

Options:
A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.
B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.
C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Answer: A

Explanation:

- A: Correct. S3 Transfer Acceleration provides fast global uploads through CloudFront edge locations. Multipart upload optimizes large file transfer. Minimal setup, low operational effort.

- B: Incorrect. Cross-Region Replication is asynchronous, creates multiple buckets, and adds unnecessary complexity.

- C: Incorrect. Snowball Edge is designed for bulk offline transfers, not daily high-speed uploads with internet available.

- D: Incorrect. EC2 + EBS snapshots introduce unnecessary costs and complexity, not scalable for continuous ingestion.

Question 502:
A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture. What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

Options:
A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.
B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.
C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.
D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

Answer: C

Explanation:

- A: Incorrect. Redshift requires ETL, loading data, and additional management overhead for simple queries.

- B: Incorrect. CloudWatch Logs is good for log monitoring/metrics, not ad-hoc SQL queries over JSON in S3.

- C: Correct. Athena queries JSON directly in S3 with no infrastructure setup, perfect for ad-hoc on-demand SQL.

- D: Incorrect. Glue + EMR is complex and costly for simple querying requirements.

Question 503:
A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations. Which solution meets these requirements with the LEAST amount of operational overhead?

Options:
A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Answer: A

Explanation:

- A: Correct. aws:PrincipalOrgID ensures only accounts in the same Org can access the bucket. Simple and scalable.

- B: Incorrect. OrgPaths is more granular and complex to manage. Not needed here.

- C: Incorrect. CloudTrail is monitoring, not enforcement of bucket access.

- D: Incorrect. Tagging individual users doesn't scale and requires heavy manual management.

Question 504:
An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet. Which solution will provide private network connectivity to Amazon S3?

Options:
A. Create a gateway VPC endpoint to the S3 bucket.
B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
C. Create an instance profile on Amazon EC2 to allow S3 access.
D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Answer: A

Explanation:

- A: Correct. A gateway VPC endpoint connects EC2 to S3 privately, avoiding internet usage.

- B: Incorrect. CloudWatch Logs doesn't provide connectivity; it's for monitoring.

- C: Incorrect. An instance profile grants permissions, but it doesn't solve private connectivity.

- D: Incorrect. API Gateway isn't needed for S3 connectivity and adds overhead.

Question 505:
A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?

Options:
A. Copy the data so both EBS volumes contain all the documents.
B. Configure the Application Load Balancer to direct a user to the server with the documents.
C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Answer: C

Explanation:

- A: Incorrect. Manually copying data between EBS volumes isn't scalable and creates consistency issues.

- B: Incorrect. Routing to one server doesn't provide shared storage, still inconsistent across users.

- C: Correct. EFS is a shared, scalable file system across AZs, ensuring all EC2s see the same data.

- D: Incorrect. Routing requests to both servers doesn't solve storage synchronization and complicates logic.

Question 506:
A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth. Which solution will meet these requirements?

Options:
A. Create an S3 bucket. Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.
B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.
C. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.
D. Set up an AWS Direct Connect connection between the on-premises network and AWS. Deploy an S3 File Gateway on premises. Create a public virtual interface (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

Answer: B

Explanation:

- A: Incorrect. Uploading 70 TB over CLI consumes heavy bandwidth, not fastest.

- B: Correct. Snowball Edge allows offline bulk transfer with minimal bandwidth usage, ideal for 70 TB.

- C: Incorrect. File Gateway is for hybrid use cases, not one-time migration at large scale.

- D: Incorrect. Direct Connect setup is time-consuming, costly, and doesn't reduce bandwidth usage.

Question 507:
A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability. Which solution meets these requirements?

Options:
A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.
B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.
D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

Answer: D

Explanation:

- A: Incorrect. Kinesis Data Analytics is for analytics, not for decoupling and scaling message delivery.

- B: Incorrect. Scaling EC2 instances still creates coupling and management overhead.

- C: Incorrect. Single shard in Kinesis cannot handle sudden spikes of 100,000 msg/sec.

- D: Correct. SNS + multiple SQS queues provides decoupling, scalability, and fan-out to many consumers.

Question 508:
A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability. How should a solutions architect design the architecture to meet these requirements?

Options:
A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.
B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.
D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.

Answer: B

Explanation:

- A: Incorrect. Scheduled scaling does not respond to unpredictable workloads.

- B: Correct. SQS decouples job coordination, and queue size drives Auto Scaling for elasticity.

- C: Incorrect. CloudTrail is for logging API calls, not job distribution.

- D: Incorrect. EventBridge is event-driven, not designed for job queue scaling.

Question 509:
A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days, the files are rarely accessed. The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues. Which solution will meet these requirements?

Options:
A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
D. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Answer: B

Explanation:

- A: Incorrect. DataSync moves data but does not extend storage or provide lifecycle management.

- B: Correct. S3 File Gateway extends storage, S3 Lifecycle handles older data to Glacier Deep Archive.

- C: Incorrect. FSx provides scalable file storage but no lifecycle tiering.

- D: Incorrect. User-side tools add overhead and do not solve lifecycle automation.

Question 510:
A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received. Which solution will meet these requirements?

Options:
A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.
B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
C. Use an API Gateway authorizer to block any requests while the application processes an order.
D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Answer: B

Explanation:

- A: Incorrect. SNS does not guarantee ordering.

- B: Correct. SQS FIFO ensures strict message ordering and exactly-once processing.

- C: Incorrect. Blocking requests via authorizer is not scalable and adds latency.

- D: Incorrect. Standard SQS does not guarantee ordering.

Question 511:
A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using usernames and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management. What should a solutions architect do to accomplish this goal?

Options:
A. Use AWS Secrets Manager. Turn on automatic rotation.
B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.
C. Create an Amazon S3 bucket to store objects encrypted with AWS KMS. Store the credential file there.
D. Create an encrypted Amazon EBS volume for each EC2 instance. Move the credential file to it.

Answer: A

Explanation:

- A: Correct. Secrets Manager securely stores credentials and supports automatic rotation for Aurora.

- B: Incorrect. Parameter Store requires custom setup for rotation with Aurora.

- C: Incorrect. S3 is not intended for secure credential storage/rotation.

- D: Incorrect. EBS encryption protects storage but does not manage credentials.

Question 512:
A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53. What should a solutions architect do to meet these requirements?

Options:
A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.
B. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Configure Route 53 to route traffic to the CloudFront distribution.
C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin. Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints. Use a custom domain name for the accelerator.
D. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Use separate domain names for static and dynamic content.

Answer: A

Explanation:

- A: Correct. CloudFront caches both static and dynamic data globally and reduces latency.

- B: Incorrect. Overcomplicates with Global Accelerator for S3 which CloudFront already handles.

- C: Incorrect. Adds unnecessary complexity with Global Accelerator.

- D: Incorrect. Splitting static and dynamic via Accelerator is not cost-efficient.

Question 513:
A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication. Configure Secrets Manager to rotate the secrets on a schedule.
B. Store the credentials as secure strings in AWS Systems Manager Parameter Store. Replicate across Regions. Configure rotation on a schedule.
C. Store the credentials in an S3 bucket with SSE. Use EventBridge to invoke a Lambda function for rotation.
D. Encrypt the credentials with KMS multi-Region keys. Store in DynamoDB global tables. Use Lambda + RDS API for rotation.

Answer: A

Explanation:

- A: Correct. Secrets Manager supports multi-Region replication and automated rotation for RDS.

- B: Incorrect. Parameter Store requires custom scripting for rotation.

- C: Incorrect. S3 + EventBridge adds unnecessary custom work.

- D: Incorrect. DynamoDB approach is overly complex and not purpose-built for credentials.

Question 514:
A company runs an ecommerce application on Amazon EC2 instances behind an ALB. The instances run in an Auto Scaling group across multiple Availability Zones. The application stores transaction data in a MySQL 8.0 database hosted on a large EC2 instance. The database performance degrades quickly as load increases. The application has more reads than writes. The company needs a solution that scales automatically and maintains high availability. Which solution will meet these requirements?

Options:
A. Use Amazon Redshift with a single node for leader and compute functionality.
B. Use Amazon RDS Single-AZ deployment with read replicas.
C. Use Amazon Aurora with Multi-AZ deployment and Aurora Auto Scaling for replicas.
D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Answer: C

Explanation:

- A: Incorrect. Redshift is for analytics, not OLTP workloads.

- B: Incorrect. RDS Single-AZ lacks HA and manual replica scaling.

- C: Correct. Aurora provides HA, Multi-AZ, and auto-scaled read replicas for unpredictable traffic.

- D: Incorrect. ElastiCache improves caching but not database durability and scaling.

Question 515:
A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. On-premises they had an inspection server that filtered and inspected traffic. Which solution will meet these requirements?

Options:
A. Use Amazon GuardDuty for traffic inspection and filtering.
B. Use Traffic Mirroring to mirror traffic from the production VPC for inspection.
C. Use AWS Network Firewall to create rules for traffic inspection and filtering in the VPC.
D. Use AWS Firewall Manager to create rules for traffic inspection and filtering in the VPC.

Answer: C

Explanation:

- A: Incorrect. GuardDuty is for threat detection, not inline filtering.

- B: Incorrect. Mirroring only copies traffic, it doesn't filter.

- C: Correct. Network Firewall inspects and filters VPC traffic in and out.

- D: Incorrect. Firewall Manager is for centralized policy management, not traffic inspection.

Question 516:
A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides visualization and includes all data sources. Only management should have full access; others should have limited access. Which solution will meet these requirements?

Options:
A. Create an analysis in Amazon QuickSight. Connect all data sources and publish dashboards. Share with IAM roles.
B. Create an analysis in Amazon QuickSight. Connect all data sources and publish dashboards. Share with users and groups.
C. Use AWS Glue crawler + ETL jobs to produce reports in S3. Use S3 bucket policies for access.
D. Use AWS Glue + Athena Federated Query to generate reports and publish them to S3.

Answer: B

Explanation:

- A: Incorrect. Sharing via IAM roles is not the standard QuickSight method.

- B: Correct. QuickSight connects multiple sources, provides dashboards, and supports access control by user/group.

- C: Incorrect. Glue jobs + S3 reports lack interactive visualization.

- D: Incorrect. Athena queries provide reporting but not dashboards with visualization.

Question 517:
A company is implementing a new business application that runs on two Amazon EC2 instances and stores documents in an S3 bucket. A solutions architect must ensure EC2 instances can access the S3 bucket. What should the solutions architect do?

Options:
A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
B. Create an IAM policy and attach it directly to the EC2 instances.
C. Create an IAM group with bucket permissions and attach it to the EC2 instances.
D. Create an IAM user with S3 permissions and attach it to the EC2 instances.

Answer: A

Explanation:

- A: Correct. IAM roles are the best practice for granting EC2 access to S3.

- B: Incorrect. Policies cannot be attached directly to instances.

- C: Incorrect. Groups cannot be attached to EC2 instances.

- D: Incorrect. Users are for humans, not EC2 instances.

Question 518:
A dev team is designing a microservice that converts large images to compressed images. A user uploads an image to S3; the service should compress and save it into another S3 bucket. Which combination of actions will meet these requirements? (Choose two.)

Options:
A. Create an SQS queue and configure S3 to send a notification to the queue when an image is uploaded.
B. Configure Lambda to poll the SQS queue. When a message is processed, delete it from the queue.
C. Configure Lambda to monitor the S3 bucket directly and keep a text file in memory of processed files.
D. Launch an EC2 instance to monitor the queue, log file names, and invoke Lambda.
E. Configure an EventBridge event to send alerts when an image is uploaded.

Answer: A, B

Explanation:

- A: Correct. S3 can notify SQS when objects are uploaded.

- B: Correct. Lambda polling SQS ensures reliable processing and retries.

- C: Incorrect. Writing filenames in memory is unreliable and not durable.

- D: Incorrect. EC2 adds unnecessary management overhead.

- E: Incorrect. EventBridge + SNS is alerting, not processing.

Question 519:

A company has a three-tier web application in a VPC. Web servers are in a public subnet, app and DB servers in private subnets. The company deployed a firewall appliance in an inspection VPC and needs all web traffic inspected before reaching web servers. Which solution meets this requirement with least overhead?

Options:

A. Create an NLB in the public subnet of the app's VPC to route traffic to the appliance.
B. Create an ALB in the public subnet of the app's VPC to route traffic to the appliance.
C. Deploy a transit gateway in the inspection VPC. Configure routes through it.
D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to forward packets to the appliance.

Answer: D

Explanation:

- A: Incorrect. NLB cannot provide seamless transparent traffic inspection.

- B: Incorrect. ALB is Layer 7, not designed for packet-level inspection.

- C: Incorrect. Transit gateway is for routing, not packet-level inline inspection.

- D: Correct. Gateway Load Balancer integrates transparently with inspection appliances.

Question 520:

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. Data is stored on EBS volumes attached to EC2 instances. Modifications in test must not affect production. The company needs consistently high I/O performance and minimum cloning time. Which solution will meet these requirements?

Options:

A. Take EBS snapshots and restore onto EC2 instance store volumes in the test environment.
B. Use Multi-Attach on production volumes and attach them to test EC2 instances.
C. Take EBS snapshots, create and initialize new EBS volumes, then attach them to test EC2 instances before restoring from snapshots.
D. Take EBS snapshots and enable Fast Snapshot Restore. Restore snapshots into new EBS volumes and attach to test EC2 instances.

Answer: D

Explanation:

- A: Incorrect. Instance store volumes are ephemeral and cannot restore from snapshots.

- B: Incorrect. Multi-Attach is limited to certain scenarios and not suitable for prod/test separation.

- C: Incorrect. Initializing EBS from snapshots is slower without Fast Snapshot Restore.

- D: Correct. Fast Snapshot Restore ensures volumes are fully initialized for immediate high I/O performance.

Question 521:

An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Use Amazon S3 to host the full website in different S3 buckets. Add Amazon CloudFront distributions. Set the S3 buckets as origins for the distributions. Store the order data in Amazon S3.

B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones. Add an Application Load Balancer (ALB) to distribute the website traffic. Add another ALB for the backend APIs. Store the data in Amazon RDS for MySQL.

C. Migrate the full application to run in containers. Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic. Store the data in Amazon RDS for MySQL.

D. Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Answer: D

Explanation:

- A: Incorrect. Entire website including backend logic cannot run on S3 alone. No transaction processing.

- B: Incorrect. Auto Scaling EC2 with RDS is scalable but has high operational overhead.

- C: Incorrect. EKS adds unnecessary operational complexity for this use case.

- D: Correct. Serverless setup with S3 + CloudFront + API Gateway + Lambda + DynamoDB gives scalability, millisecond latency, and minimal ops.

Question 522:

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files. Which storage option meets these requirements?

Options:
A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Explanation:

- A: Incorrect. Provides high durability but higher cost for rarely accessed data.

- B: Correct. Intelligent-Tiering automatically optimizes costs between frequent and infrequent tiers without operational overhead.

- C: Incorrect. Standard-IA needs lifecycle rules; not efficient for unpredictable access patterns.

- D: Incorrect. One Zone-IA is cheaper but not resilient to AZ loss.

Question 523:

A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely. Which storage solution will meet these requirements MOST cost-effectively?

Options:
A. Configure S3 Intelligent-Tiering to automatically migrate objects.
B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

Answer: B

Explanation:

- A: Incorrect. Intelligent-Tiering charges monitoring fees and is unnecessary when access pattern is predictable.

- B: Correct. Glacier Deep Archive is the cheapest option for long-term archival with rare retrieval.

- C: Incorrect. Standard-IA still incurs higher storage cost compared to Deep Archive for indefinite retention.

- D: Incorrect. One Zone-IA is not suitable for indefinite storage and offers less durability than Glacier options.

Question 524:

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling. How should the solutions architect generate the information with the LEAST operational overhead?

Options:

A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Answer: B

Explanation:

- A: Incorrect. Budgets are for alerts and tracking against thresholds, not detailed historical analysis.

- B: Correct. Cost Explorer provides detailed filtering and visualization with minimal setup.

- C: Incorrect. Billing dashboard graphs are high level and lack granular filtering for instance types.

- D: Incorrect. CUR + QuickSight works but requires additional setup and is more complex.

Question 525:

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database. During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort. Which solution will meet these requirements?

Options:

A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.
B. Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: D

Explanation:

- A: Incorrect. Moving to EC2 adds ops overhead and reduces scalability.

- B: Incorrect. DynamoDB is not equivalent to Aurora, and switching DB engines is not required.

- C: Incorrect. SNS does not guarantee reliable message delivery order and retry for DB writes.

- D: Correct. Using SQS decouples ingestion from database writes, improves scalability, and minimizes Lambda concurrency limits.

Question 526:
A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes.

Options:
A. Turn on AWS Config with the appropriate rules.
B. Turn on AWS Trusted Advisor with the appropriate checks.
C. Turn on Amazon Inspector with the appropriate assessment template.
D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon CloudWatch Events).

Answer: A

Explanation:

- A: Correct. AWS Config continuously monitors S3 configuration changes and can alert/remediate unauthorized changes.

- B: Incorrect. Trusted Advisor provides recommendations but not continuous monitoring.

- C: Incorrect. Inspector is for vulnerability/security assessments, not bucket config monitoring.

- D: Incorrect. Logging provides activity history but not prevention/detection of unauthorized configuration changes.

Question 527:
A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege. Which solution will meet these requirements?

Options:
A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
B. Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.
C. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Answer: A

Explanation:

- A: Correct. CloudWatch dashboard sharing allows external access via a secure URL without an AWS account.

- B: Incorrect. Creating IAM users for external parties violates best practices and adds overhead.

- C: Incorrect. Same as B, still requires AWS account and access management.

- D: Incorrect. Overly complex and insecure just to share a dashboard.

Question 528:
A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory. Which solution will meet these requirements?

Options:
A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Answer: B

Explanation:

- A: Incorrect. One-way trust does not allow full SSO capability across all accounts.

- B: Correct. AWS SSO with two-way trust provides seamless integration with on-prem AD for central management.

- C: Incorrect. Directory Service alone does not provide SSO across AWS accounts.

- D: Incorrect. Running on-prem IdP adds overhead when AWS SSO already integrates with AD.

Question 529:
A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions. The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions. Which solution will meet these requirements?

Options:
A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.
B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.
C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.
D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Answer: A

Explanation:

- A: Correct. NLB supports UDP, Global Accelerator provides latency-based routing and automated failover.

- B: Incorrect. ALB does not support UDP.

- C: Incorrect. Route 53 latency records help but CloudFront does not support UDP traffic.

- D: Incorrect. Weighted records don't guarantee lowest latency; ALB still doesn't support UDP.

Question 530:
A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance. Which solution meets these requirements MOST cost-effectively?

Options:
A. Stop the DB instance when tests are completed. Restart the DB instance when required.
B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

Answer: C

Explanation:

- A: Incorrect. Stopping an RDS instance still incurs storage costs, and not suitable for monthly use.

- B: Incorrect. RDS does not support Auto Scaling of instance size.

- C: Correct. Creating a snapshot and restoring only when needed minimizes costs while keeping performance.

- D: Incorrect. Manually resizing instance adds ops overhead and still incurs ongoing costs.

Question 531:
A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this?

Options:
A. Use AWS Config rules to define and detect resources that are not properly tagged.
B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Answer: A

Explanation:

- A: Correct. AWS Config has managed rules for tag compliance and requires minimal effort.

- B: Incorrect. Cost Explorer is for cost allocation, not for enforcing tagging compliance.

- C: Incorrect. Custom scripts add unnecessary operational overhead.

- D: Incorrect. Similar to C, manual Lambda/API approach requires maintenance.

Question 532:

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images. Which method is the MOST cost-effective for hosting the website?

Options:

A. Containerize the website and host it in AWS Fargate.

B. Create an Amazon S3 bucket and host the website there.

C. Deploy a web server on an Amazon EC2 instance to host the website.

D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Answer: B

Explanation:

- A: Incorrect. Fargate adds unnecessary compute cost for static content.

- B: Correct. S3 static website hosting is the cheapest and simplest for static files.

- C: Incorrect. EC2 incurs higher cost and operational management.

- D: Incorrect. ALB + Lambda is expensive and overkill for static content.

Question 533:

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval. What should a solutions architect recommend to meet these requirements?

Options:

A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.

B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.

C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.

D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Answer: C

Explanation:

- A: Incorrect. DynamoDB cannot apply rules to strip sensitive data on write.

- B: Incorrect. Kinesis Firehose delivers data but is not suitable for multi-consumer near-real-time use cases.

- C: Correct. Kinesis Data Streams + Lambda preprocessing allows sensitive data removal and multiple consumers with real-time scalability.

- D: Incorrect. S3 batch processing introduces delay and is not near-real-time.

Question 534:
A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources. What should a solutions architect do to meet these requirements?

Options:
A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.
B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.
C. Use Amazon CloudWatch to monitor API calls. Use Amazon EventBridge (Amazon CloudWatch Events) to record resource configuration changes.
D. Use AWS Systems Manager to track configuration changes and AWS Trusted Advisor to record API calls.

Answer: B

Explanation:

- A: Incorrect. CloudTrail does not track resource configuration changes; it tracks API calls.

- B: Correct. Config tracks configuration changes, CloudTrail records API calls — together they provide full compliance tracking.

- C: Incorrect. CloudWatch/EventBridge are not meant for historical auditing of API/configuration.

- D: Incorrect. Systems Manager and Trusted Advisor do not fulfill compliance history requirements.

Question 535:
A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website. Which solution meets these requirements MOST cost-effectively?

Options:
A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Answer: C

Explanation:

- A: Incorrect. Replicating to all Regions is expensive and complex.

- B: Incorrect. Global Accelerator is not cost-effective for static content use case.

- C: Correct. CloudFront caches content globally at edge locations, reducing latency at low cost.

- D: Incorrect. S3 Transfer Acceleration improves upload speed, not global delivery latency.

Question 536:
A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website. The company has noticed that some insert operations are taking 10 seconds or longer. The company has determined that the database storage performance is the problem. Which solution addresses this performance issue?

Options:
A. Change the storage type to Provisioned IOPS SSD.
B. Change the DB instance to a memory optimized instance class.
C. Change the DB instance to a burstable performance instance class.
D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Answer: A

Explanation:

- A: Correct. Provisioned IOPS SSD provides consistent, high-performance storage needed for heavy inserts.

- B: Incorrect. Memory optimization helps with caching/queries but not storage write bottlenecks.

- C: Incorrect. Burstable performance is not designed for sustained heavy workloads.

- D: Incorrect. Read replicas help read scalability, not write performance.

Question 537:
A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis. The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days. What is the MOST operationally efficient solution that meets these requirements?

Options:
A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.
D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Answer: A

Explanation:

- A: Correct. Firehose to S3 is serverless, HA, low-cost, and lifecycle policies handle archival.

- B: Incorrect. EC2 ingestion requires infrastructure management and scaling.

- C: Incorrect. OpenSearch is expensive and not needed for all alerts.

- D: Incorrect. SQS retention max is 14 days, no automatic archiving to S3.

Question 538:

A company's application integrates with multiple SaaS sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible. Which solution will meet these requirements with the LEAST operational overhead?

Options:

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

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

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

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

Answer: B

Explanation:

- A: Incorrect. Still relies on EC2, increasing ops overhead.

- B: Correct. AppFlow directly integrates SaaS to S3, serverless, low ops. SNS for notifications ensures performance.

- C: Incorrect. EventBridge cannot directly pull from SaaS data sources.

- D: Incorrect. ECS adds more infrastructure complexity compared to AppFlow.

Question 539:

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

Options:

A. Launch the NAT gateway in each Availability Zone.
B. Replace the NAT gateway with a NAT instance.
C. Deploy a gateway VPC endpoint for Amazon S3.
D. Provision an EC2 Dedicated Host to run the EC2 instances.

Answer: C

Explanation:

- A: Incorrect. Multiple NAT gateways still incur data transfer charges to S3.

- B: Incorrect. NAT instance has same data transfer costs as NAT gateway.

- C: Correct. Gateway VPC endpoint enables private connectivity to S3 without data transfer charges.

- D: Incorrect. Dedicated Hosts are unrelated to S3 data transfer optimization.

Question 540:
A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and minimal impact on internet connectivity for internal users. Which solution meets these requirements?

Options:
A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
C. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.
D. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

Answer: B

Explanation:

- A: Incorrect. VPN does not solve bandwidth issues; still uses internet.

- B: Correct. Direct Connect provides dedicated, consistent bandwidth for backups without affecting internet usage.

- C: Incorrect. Daily Snowball use is impractical and slow for time-sensitive data.

- D: Incorrect. Removing service limits does not resolve bandwidth bottleneck.

Question 541:
A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion. Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

Options:
A. Enable versioning on the S3 bucket.
B. Enable MFA Delete on the S3 bucket.
C. Create a bucket policy on the S3 bucket.
D. Enable default encryption on the S3 bucket.
E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: A, B

Explanation:

- A: Correct. Versioning protects against accidental deletion by keeping object versions.

- B: Correct. MFA Delete requires additional authentication for delete operations.

- C: Incorrect. Bucket policies help with access, not deletion protection.

- D: Incorrect. Encryption protects data confidentiality, not deletion.

- E: Incorrect. Lifecycle policies are for data transition/expiration, not deletion prevention.

Question 542:
A company has a data ingestion workflow that consists of the following:
• An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
• An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job. Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

Options:
A. Deploy the Lambda function in multiple Availability Zones.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.
C. Increase the CPU and memory that are allocated to the Lambda function.
D. Increase provisioned throughput for the Lambda function.
E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: B, E

Explanation:

- A: Incorrect. Lambda is automatically multi-AZ; redeploying doesn't fix message durability.

- B: Correct. Subscribing SQS to SNS ensures durable message storage.

- C: Incorrect. Increasing CPU/memory does not address message loss.

- D: Incorrect. Provisioned throughput is not relevant for failed message ingestion.

- E: Correct. Lambda polling from SQS guarantees retries and prevents data loss.

Question 543:

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

Options:

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

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

C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon SNS to trigger notifications.

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

Answer: B

Explanation:

- A: Incorrect. Inspector does not scan S3 for PII.

- B: Correct. Macie natively detects PII in S3 and integrates with SNS for notifications.

- C: Incorrect. Custom Lambda adds unnecessary development effort compared to Macie.

- D: Incorrect. Same as C, more complex and not efficient.

Question 544:
A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week. What should the company do to guarantee the EC2 capacity?

Options:
A. Purchase Reserved Instances that specify the Region needed.
B. Create an On-Demand Capacity Reservation that specifies the Region needed.
C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

Answer: D

Explanation:

- A: Incorrect. Reserved Instances provide cost savings, not guaranteed capacity.

- B: Incorrect. Region-only reservation does not guarantee AZ-specific capacity.

- C: Incorrect. Reserved Instances don't guarantee AZ capacity availability.

- D: Correct. On-Demand Capacity Reservation with AZs ensures capacity in chosen AZs.

Question 545:
A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and stored in a durable location. What should a solutions architect do to meet these requirements?

Options:
A. Move the catalog to Amazon ElastiCache for Redis.
B. Deploy a larger EC2 instance with a larger instance store.
C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Answer: D

Explanation:

- A: Incorrect. ElastiCache is not for durable, persistent storage.

- B: Incorrect. Larger instance store is still ephemeral and not durable.

- C: Incorrect. Glacier is for archival, not active use.

- D: Correct. EFS is durable, scalable, and highly available across AZs.

Question 546:
A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1 year old as quickly as possible. A delay in retrieving older files is acceptable. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files.
B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve files from S3 directly; use Glacier Select for archived files.
C. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move files to S3 Glacier Instant Retrieval after 1 year. Query metadata in S3 to retrieve archived files.
D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS.

Answer: B

Explanation:

- A: Incorrect. Glacier Instant Retrieval is costlier than Intelligent-Tiering for frequent access within 1 year.

- B: Correct. Intelligent-Tiering optimizes cost for active files; Glacier Flexible Retrieval is best for >1 year archive.

- C: Incorrect. Glacier Instant Retrieval after 1 year is more expensive than Flexible Retrieval.

- D: Incorrect. Glacier Deep Archive is too slow for even occasional queries.

Question 547:
A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability. What should a solutions architect do to meet these requirements?

Options:
A. Create an AWS Lambda function to apply the patch to all EC2 instances.
B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Answer: D

Explanation:

- A: Incorrect. Lambda cannot patch EC2 OS or software directly.

- B: Incorrect. Patch Manager is for OS and AWS-managed patches, not third-party software.

- C: Incorrect. Maintenance window still relies on Patch Manager, not suitable for custom software.

- D: Correct. Run Command lets you push custom commands/scripts to patch all instances quickly.

uestion 548:

A company needs to run analytics on data that is stored in Amazon S3. The data size is several terabytes and grows continuously. The company requires a solution that provides interactive queries with minimal infrastructure management. Which solution should a solutions architect recommend?

Options:
A. Load the data into Amazon Redshift and run queries using Amazon Redshift Spectrum.
B. Use Amazon Athena to run queries directly on the data stored in S3.
C. Use AWS Glue to transform the data and load it into Amazon RDS for querying.
D. Deploy a Hadoop cluster on Amazon EC2 instances to run queries.

Answer: B

Explanation:

- A: Incorrect. Redshift is powerful but requires cluster management and additional cost.

- B: Correct. Athena provides serverless, interactive queries directly on S3 data with minimal management.

- C: Incorrect. RDS is not designed for large-scale analytics workloads.

- D: Incorrect. Hadoop on EC2 is complex and has high operational overhead.

Question 549:
A company has an ecommerce application that stores order data in Amazon RDS for PostgreSQL. The application experiences unpredictable traffic and the read queries are becoming a bottleneck. The company needs a highly available solution that can automatically scale to handle the unpredictable read traffic without manual intervention. Which solution meets these requirements?

Options:
A. Use Amazon RDS in Multi-AZ mode with provisioned IOPS.
B. Use Amazon RDS read replicas and manually add/remove replicas based on traffic.
C. Use Amazon Aurora with Aurora Replicas and enable Aurora Auto Scaling.
D. Migrate the database to Amazon DynamoDB with on-demand capacity mode.

Answer: C

Explanation:

- A: Incorrect. Multi-AZ provides HA for writes, not read scaling.

- B: Incorrect. Read replicas help, but scaling is manual and not automatic.

- C: Correct. Aurora Replicas + Auto Scaling provide HA and automatic scaling for unpredictable read traffic.

- D: Incorrect. DynamoDB is a different database engine; migration is unnecessary.

Question 550:
A company's security team requires that all new Amazon S3 objects be encrypted at rest upon creation. The solution must not require developers to make any application changes. Which solution should a solutions architect recommend?

Options:
A. Enable default encryption on the S3 bucket.
B. Create an S3 Lifecycle policy to encrypt objects after creation.
C. Use AWS Key Management Service (AWS KMS) to encrypt the objects before uploading them.
D. Attach a bucket policy that denies upload requests without encryption headers.

Answer: A

Explanation:

- A: Correct. Default encryption ensures all new objects are automatically encrypted at rest without application changes.

- B: Incorrect. Lifecycle policies cannot retroactively encrypt unencrypted objects.

- C: Incorrect. Requires developers to modify applications to use KMS APIs.

- D: Incorrect. Deny policies would block uploads without headers, requiring application changes.

Question 551:
A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning. Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

Options:
A. Configure the application to send the data to Amazon Kinesis Data Firehose.
B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

Answer: B, D

Explanation:

- A: Incorrect. Kinesis Firehose is for streaming ingestion, not scheduled reporting.

- B: Correct. SES can format and send emails reliably.

- C: Incorrect. Glue is for ETL jobs, not suitable for simple queries and scheduling HTML reporting.

- D: Correct. EventBridge + Lambda can schedule the daily data extraction.

- E: Incorrect. S3 events are triggered on object creation, not for daily scheduled reporting.

Question 552:
A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead. Which solution will meet these requirements?

Options:
A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.
B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.
C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

Answer: C

Explanation:

- A: Incorrect. S3 is object storage, not a POSIX file system.

- B: Incorrect. EBS is block storage, not scalable across AZs or multiple instances.

- C: Correct. EFS is fully managed, highly available, auto-scaling, and supports standard file system structure.

- D: Incorrect. EBS cannot scale automatically and is tied to single instances/AZ.

Question 553:

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency. Which solution will meet these requirements?

Options:

A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.
B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.
C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.
D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Answer: C

Explanation:

- A: Incorrect. Glacier storage class only is not suitable because records must be immediately accessible for 1 year.

- B: Incorrect. IAM policies can be changed; they do not guarantee compliance-level protection.

- C: Correct. Lifecycle policy + Object Lock compliance mode ensures WORM (write once, read many) with maximum resiliency.

- D: Incorrect. Governance mode can be overridden by administrators; compliance mode is required.

Question 554:

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files. What should a solutions architect do to meet these requirements?

Options:

A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.
B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.
C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.
D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Answer: C

Explanation:

- A: Incorrect. S3 does not natively support Windows SMB shares.

- B: Incorrect. S3 File Gateway is NFS/SMB but not optimized for full Windows AD integration.

- C: Correct. FSx for Windows File Server supports native SMB, AD integration, HA, and durability.

- D: Incorrect. EFS supports NFS, not SMB for Windows file sharing.

Question 555:
A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases. Which solution will meet these requirements?

Options:
A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.
B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Answer: C

Explanation:

- A: Incorrect. Route tables cannot restrict access at the subnet-to-subnet security group level.

- B: Incorrect. Security groups do not use "deny" rules, they only allow traffic.

- C: Correct. Security groups allowing inbound traffic only from private subnet instances meet the requirement.

- D: Incorrect. Peering is for VPC-to-VPC communication, not within the same VPC.

Question 556:

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

Options:

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

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

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

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

Answer: C

Explanation:

- A: Incorrect. Stage variables do not support custom domain names with SSL/TLS certificates.

- B: Incorrect. Certificates must be in the same Region as the API Gateway. us-east-1 is not valid here.

- C: Correct. Custom domain + ACM certificate in the same Region allows HTTPS with Route 53 alias.

- D: Incorrect. Certificate region mismatch makes this invalid.

Question 557:

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

Options:

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

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

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

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

Answer: B

Explanation:

- A: Incorrect. Comprehend analyzes text, not images.

- B: Correct. Rekognition has pre-built moderation APIs to detect inappropriate image content.

- C: Incorrect. SageMaker requires building and training custom models, more effort.

- D: Incorrect. Fargate deployment adds operational overhead for custom ML.

Question 558:
A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload. What should a solutions architect do to meet these requirements?

Options:
A. Use Amazon EC2 instances, and install Docker on the instances.
B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Answer: C

Explanation:

- A: Incorrect. Running Docker on EC2 requires full infra management.

- B: Incorrect. ECS on EC2 still requires cluster and capacity management.

- C: Correct. ECS on Fargate is fully serverless; AWS manages infrastructure.

- D: Incorrect. ECS-optimized AMIs still require provisioning and scaling EC2.

Question 559:
A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day. What should a solutions architect do to transmit and process the clickstream data?

Options:
A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Answer: D

Explanation:

- A: Incorrect. Data Pipeline is outdated and not suitable for real-time data streaming.

- B: Incorrect. EC2 scaling for 30 TB/day adds huge operational overhead.

- C: Incorrect. CloudFront caching is unrelated to data ingestion/processing.

- D: Correct. Kinesis Data Streams + Firehose handles real-time ingestion and delivery to S3/Redshift at scale.

Question 560:
A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS. What should a solutions architect do to meet this requirement?

Options:
A. Update the ALB's network ACL to accept only HTTPS traffic.
B. Create a rule that replaces the HTTP in the URL with HTTPS.
C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer: C

Explanation:

- A: Incorrect. Network ACLs cannot redirect traffic, only allow/deny.

- B: Incorrect. Rules cannot directly rewrite URLs in ALB.

- C: Correct. ALB listener rule supports HTTP-to-HTTPS redirection natively.

- D: Incorrect. NLB doesn't operate at Layer 7 and cannot handle HTTPS redirection.

Question 561:
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.
C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

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

Answer: C

Explanation:

- A: Incorrect. Storing credentials in metadata is insecure and requires manual management.

- B: Incorrect. S3 requires additional automation for rotation; not minimal overhead.

- C: Correct. Secrets Manager natively rotates credentials with least effort.

- D: Incorrect. Parameter Store does not support automatic rotation for RDS credentials.

Question 562:
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires. What should a solutions architect do to meet these requirements?

Options:
A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Answer: D

Explanation:

- A: Incorrect. ACM-managed certs are only for Amazon-issued certs, not external.

- B: Incorrect. Importing external certs into ACM does not allow managed rotation.

- C: Incorrect. Private CA issues internal certs, not for external authority requirements.

- D: Correct. Imported certs must be rotated manually; EventBridge helps track expiry.

Question 563:
A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time. Which solution meets these requirements MOST cost-effectively?

Options:
A. Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.
B. Save the .pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.
C. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and the .jpg files in the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

Answer: A

Explanation:

- A: Correct. S3 + Lambda is serverless, cost-effective, and scales automatically.

- B: Incorrect. DynamoDB is not designed for large binary files like PDFs/images.

- C: Incorrect. Elastic Beanstalk + EC2 adds unnecessary cost and management overhead.

- D: Incorrect. Same overhead issue as C; not cost-optimized.

Question 564:
A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day. The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS. What should a solutions architect do to meet these requirements?

Options:
A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.
B. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to the S3 File Gateway. Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.
C. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.

D. Deploy and configure Amazon FSx for Windows File Server on AWS. Deploy and configure an Amazon FSx File Gateway on premises. Move the on-premises file data to the FSx File Gateway. Configure the cloud workloads to use FSx for Windows File Server on AWS. Configure the on-premises workloads to use the FSx File Gateway.

Answer: D

Explanation:

- A: Incorrect. Would require reconfiguring all on-premises workloads to AWS FSx directly.

- B: Incorrect. S3 File Gateway is not native Windows SMB; not ideal for existing access patterns.

- C: Incorrect. S3 is object storage; workloads expect SMB/NFS compatibility.

- D: Correct. FSx + FSx File Gateway provides hybrid file storage, native SMB access, minimal changes.

Question 565:
A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.
C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
D. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Answer: C

Explanation:

- A: Incorrect. Custom libraries add heavy dev and maintenance overhead.

- B: Incorrect. SageMaker requires custom training; unnecessary for PHI detection.

- C: Correct. Textract extracts text; Comprehend Medical identifies PHI automatically with minimal effort.

- D: Incorrect. Rekognition is for images/labels, not text extraction from documents.

Question 566:

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

Options:

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

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

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

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

Answer: C

Explanation:

- A: Incorrect. Glacier does not provide immediate access.

- B: Incorrect. One Zone-IA sacrifices resiliency; not suitable for critical data.

- C: Correct. S3 Standard-IA is cost-effective, resilient, and allows immediate access after 30 days.

- D: Incorrect. Glacier does not allow fast retrieval, so not suitable.

Question 567:

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

Options:

A. Use the CreateQueue API call to create a new queue.
B. Use the AddPermission API call to add appropriate permissions.
C. Use the ReceiveMessage API call to set an appropriate wait time.
D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Answer: D

Explanation:

- A: Incorrect. Creating a new queue does not solve duplicate processing.

- B: Incorrect. Permissions are not related to duplicate message processing.

- C: Incorrect. Wait time reduces empty responses but not duplicates.

- D: Correct. Increasing visibility timeout prevents multiple consumers from reprocessing the same message.

Question 568:
A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails. What should the solutions architect do to meet these requirements?

Options:
A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Answer: A

Explanation:

- A: Correct. Direct Connect for primary low-latency + VPN as backup = cost-effective and HA.

- B: Incorrect. VPN-only solution is cheaper but does not meet low-latency requirement.

- C: Incorrect. Dual Direct Connect is more costly; not minimal cost.

- D: Incorrect. Failover attribute is not an automatic provisioning mechanism.

Question 569:
A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data. Which solution will meet these requirements with the LEAST operational effort?

Options:
A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.
B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.
D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Answer: B

Explanation:

- A: Incorrect. Multi-Region is overkill, complex, and adds latency.

- B: Correct. Multi-AZ Auto Scaling + Multi-AZ Aurora ensures HA with minimal effort.

- C: Incorrect. Snapshot recovery causes downtime and data loss.

- D: Incorrect. Writing through S3 adds latency and complexity.

Question 570:
A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service. The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code. What should a solutions architect do to meet these requirements?

Options:
A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
D. Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Answer: C

Explanation:

- A: Incorrect. NLB supports TCP health checks only, not HTTP.

- B: Incorrect. Cron jobs add management overhead and complexity.

- C: Correct. ALB supports HTTP health checks and Auto Scaling replacement of unhealthy instances.

- D: Incorrect. CloudWatch alarms cannot inspect HTTP response codes directly.

Question 571:
A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour. What should the solutions architect recommend to meet these requirements?

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

Answer: B

Explanation:

- A: Incorrect. Global tables are for multi-region replication, not RPO recovery.

- B: Correct. Point-in-time recovery enables restoring DynamoDB within 15-minute RPO.

- C: Incorrect. Glacier recovery is too slow; cannot meet RTO.

- ~~D: Incorrect. DynamoDB does not use EBS snapshots.~~

Question 572:
A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs. How can the solutions architect meet this requirement?

Options:
A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.
C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.
D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Answer: D

Explanation:

- A: Incorrect. API Gateway is not used for direct S3 traffic.

- B: Incorrect. NAT incurs costs and still uses internet path.

- C: Incorrect. Using internet gateway still incurs data transfer charges.

- D: Correct. Gateway endpoint enables private S3 access without transfer costs.

Question 573:
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access. Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

Options:
A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Answer: C, D

Explanation:

- A: Incorrect. Bastion host must allow company users, not app instances.

- B: Incorrect. Internal IP range is not relevant; need external IP for company network.

- C: Correct. Bastion host must allow SSH from company external IP range.

- D: Correct. Application instances should only allow SSH from bastion's private IP.

- E: Incorrect. Public IP of bastion is not used inside private subnet.

Question 574:

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

Options:

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Answer: A, C

Explanation:

- A: Correct. Web tier must allow HTTPS traffic from the internet.

- B: Incorrect. Outbound 443 is not required; defaults allow all outbound.

- C: Correct. Database tier must allow SQL traffic (1433) from web tier.

- D: Incorrect. Database does not initiate outbound to web.

- E: Incorrect. Allowing both ports unnecessarily increases exposure.

Question 575:

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

Options:

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.

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

Answer: A

Explanation:

- A: Correct. API Gateway + Lambda + SQS provides loosely coupled, scalable, and modernized architecture.

- B: Incorrect. Scaling EC2 vertically doesn't solve overload or modernization.

- C: Incorrect. SNS alone is push-based, not suitable for REST API request buffering.

- D: Incorrect. While SQS helps, keeping EC2 adds operational burden compared to serverless.

Question 576:
A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive. Which solution offers the MOST reliable data transfer?

Options:
A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer: B

Explanation:

- A: Incorrect. DataSync over public internet is less secure and less reliable.

- B: Correct. DataSync over Direct Connect ensures secure, reliable, large-scale transfer.

- C: Incorrect. DMS is for database replication, not file transfer.

- D: Incorrect. Same reason as C, wrong service.

Question 577:
A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.

Answer: C

Explanation:

- A: Incorrect. EC2 adds unnecessary management overhead.

- B: Incorrect. AWS Glue is not designed for real-time streaming ingestion.

- C: Correct. API Gateway + Kinesis + Firehose + Lambda provides fully managed real-time pipeline.

- D: Incorrect. Glue is for batch ETL, not real-time.

Question 578:
A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years. What is the MOST operationally efficient solution that meets these requirements?

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

Answer: B

Explanation:

- A: Incorrect. Point-in-time recovery allows restore, not long-term retention.

- B: Correct. AWS Backup manages schedules and long-term retention with minimal effort.

- C: Incorrect. On-demand backups require manual effort.

- D: Incorrect. Custom Lambda adds unnecessary operational burden.

Question 579:
A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly. What should a solutions architect recommend?

Options:
A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A

Explanation:

- A: Correct. On-demand mode is best for unpredictable and spiky workloads.

- B: Incorrect. GSI improves query flexibility, not cost optimization.

- C: Incorrect. Auto scaling lags behind sudden spikes.

- D: Incorrect. Global tables are for multi-region replication, not cost savings.

Question 580:
A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots. What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

Options:
A. Make the encrypted AMI and snapshots publicly available. Modify the key policy to allow the MSP Partner's AWS account to use the key.
B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key.
C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to trust a new KMS key that is owned by the MSP Partner for encryption.
D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account. Encrypt the S3 bucket with a new KMS key that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

Answer: B

Explanation:

- A: Incorrect. Making AMI public is insecure.

- B: Correct. Sharing AMI privately + updating key policy is secure and appropriate.

- C: Incorrect. Requires re-encryption; unnecessary complexity.

- D: Incorrect. Exporting/importing AMIs is less efficient.

Question 581:
A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

Options:
A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.

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

Answer: C

Explanation:

- A: Incorrect. SNS is pub/sub, not suitable for job queue durability.

- B: Incorrect. Scaling on network usage is not tied to job volume.

- C: Correct. SQS ensures durability + scaling on queue length matches workload.

- D: Incorrect. SNS does not persist messages like SQS.

Question 582:
A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate. What should a solutions architect recommend to meet this requirement?

Options:
A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.
B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
C. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

Answer: B

Explanation:

- A: Incorrect. ACM has no such rule to publish custom messages.

- B: Correct. AWS Config monitors certificate expiration and integrates with EventBridge + SNS.

- C: Incorrect. Trusted Advisor checks require Business/Enterprise support and not real-time.

- D: Incorrect. EventBridge cannot directly detect ACM expiration without Config.

Question 583:
A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed. What should the solutions architect recommend?

Options:
A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
B. Move the website to Amazon S3. Use Cross-Region Replication between Regions.
C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers.

Answer: C

Explanation:

- A: Incorrect. Moving site to US AWS region doesn't help EU latency.

- B: Incorrect. Cross-Region replication not relevant here.

- C: Correct. CloudFront caches static/dynamic content closer to EU users.

- D: Incorrect. Route 53 routing still resolves to US servers.

Question 584:
A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours. The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use. Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

Options:
A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.
C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
D. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

Answer: B

Explanation:

- A: Incorrect. Spot not suitable for production as it can be interrupted.

- B: Correct. RIs for production (always running) + On-Demand with automation for dev/test.

- C: Incorrect. Spot blocks not cost-efficient or reliable for production.

- D: Incorrect. On-Demand for production is costlier.

Question 585:
A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored. What should a solutions architect do to meet this requirement?

Options:
A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Answer: A

Explanation:

- A: Correct. Object Lock (compliance mode) ensures immutability.

- B: Incorrect. Lifecycle policy doesn't prevent modification/deletion.

- C: Incorrect. ACL doesn't guarantee immutability.

- D: Incorrect. EFS read-only mode is reversible; not compliant.

Question 586:
A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. Which solution meets these requirements?

Options:
A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Answer: A

Explanation:

- A: Correct. Secrets Manager rotates credentials automatically and securely.

- B: Incorrect. OpsCenter is not meant for secret storage.

- C: Incorrect. S3 is not designed for credential rotation.

- D: Incorrect. Manual management of credentials adds overhead.

Question 587:
A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the events. A solutions architect needs to design a solution that stores customer data that is created during database upgrades. Which solution will meet these requirements?

Options:
A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Answer: D

Explanation:

- A: Incorrect. RDS Proxy helps with connection pooling, not during full DB downtime.

- B: Incorrect. Extending runtime and retries won't guarantee persistence.

- C: Incorrect. Lambda local storage is ephemeral and unreliable.

- D: Correct. SQS ensures durability; retries data after DB upgrade.

Question 588:
A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible. Which solution will meet these requirements?

Options:
A. Configure the Requester Pays feature on the company's S3 bucket.
B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Answer: A

Explanation:

- A: Correct. Requester Pays shifts cost of access to the marketing firm.

- B: Incorrect. Cross-region replication incurs additional replication cost.

- C: Incorrect. Cross-account access still charges data transfer fees to the owner.

- D: Incorrect. Intelligent-Tiering is about storage class, not transfer cost.

Question 589:
A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution. What should a solutions architect do to secure the audit documents?

Options:
A. Enable the versioning and MFA Delete features on the S3 bucket.
B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

Explanation:

- A: Correct. Versioning + MFA Delete protects against accidental/malicious deletions.

- B: Incorrect. MFA on users is not related to object deletion protection.

- C: Incorrect. Lifecycle policies do not control IAM permissions.

- D: Incorrect. KMS encryption does not prevent deletion.

Question 590:
A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours. The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue. Which solution will meet this requirement with the LEAST operational overhead?

Options:
A. Modify the DB instance to be a Multi-AZ deployment.
B. Create a read replica of the database. Configure the script to query only the read replica.
C. Instruct the development team to manually export the entries in the database at the end of each day.
D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

Answer: B

Explanation:

- A: Incorrect. Multi-AZ adds availability but not read performance.

- B: Correct. Read replica offloads read queries from primary DB.

- C: Incorrect. Manual export adds operational overhead.

- D: Incorrect. ElastiCache helps for frequently repeated queries, not full table scans.

Question 591:
A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet. Which solution will meet these requirements?

Options:
A. Configure an S3 gateway endpoint.
B. Create an S3 bucket in a private subnet.
C. Create an S3 bucket in the same AWS Region as the EC2 instances.
D. Configure a NAT gateway in the same subnet as the EC2 instances.

Answer: A

Explanation:

- A: Correct. Gateway endpoint enables private communication with S3.

- B: Incorrect. S3 is a regional service, not confined to a subnet.

- C: Incorrect. Same Region still goes via internet without endpoint.

- D: Incorrect. NAT uses internet path, violating requirement.

Question 592:
A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC. Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

Options:
A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
B. Create a bucket policy to make the objects in the S3 bucket public.
C. Create a bucket policy that limits access to only the application tier running in the VPC.
D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Answer: A, C

Explanation:

- A: Correct. VPC endpoint ensures private access to S3.

- B: Incorrect. Public bucket violates security requirements.

- C: Correct. Bucket policy restricting access to VPC enhances security.

- D: Incorrect. Hardcoding credentials is insecure.

- E: Incorrect. NAT uses internet path.

Question 593:
A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability. The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes. A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay. Which solution meets these requirements?

Options:
A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Answer: B

Explanation:

- A: Incorrect. Backup/restore adds latency and delays staging.

- B: Correct. Aurora cloning creates staging copies instantly without performance impact.

- C: Incorrect. Standby is not for reads; only failover.

- D: Incorrect. mysqldump again causes latency and overhead.

Question 594:
A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis. Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files. Which solution meets these requirements with the LEAST operational overhead?

Options:
A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.
B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

Answer: C

Explanation:

- A: Incorrect. EMR is too heavy for small, one-time processing.

- B: Incorrect. EC2 requires manual scaling and more ops overhead.

- C: Correct. S3 event → SQS → Lambda provides fully managed scaling.

- D: Incorrect. EventBridge + Kinesis adds unnecessary complexity.

Question 595:
An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly. What should the solutions architect recommend?

Options:
A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Answer: D

Explanation:

- A: Incorrect. Multi-AZ improves HA, not read performance.

- B: Incorrect. Secondary in Multi-AZ is standby, not for reads.

- C: Incorrect. Smaller replicas may not handle load.

- D: Correct. Full-sized replicas handle read traffic effectively.

Question 596:
An Amazon EC2 administrator created the following policy associated with an IAM group containing several users: (policy omitted here). What is the effect of this policy?

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

Answer: C

Explanation:

- A: Incorrect. Policy restricts based on IP, not region-wide exception.

- B: Incorrect. IP is not of instance, but source IP of request.

- C: Correct. Condition explicitly allows terminate only if source IP = 10.100.100.254.

- D: Incorrect. Opposite of correct interpretation.

Question 597:
A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control. Which solution will satisfy these requirements?

Options:
A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Answer: D

Explanation:

- A: Incorrect. EFS is NFS, not SMB for Windows.

- B: Incorrect. Storage Gateway is not highly available across AZs.

- C: Incorrect. S3 cannot natively be mounted as SMB.

- D: Correct. FSx for Windows provides SMB + AD integration + HA.

Question 598:
An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email. Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages. What should the solutions architect do to resolve this issue with the LEAST operational overhead?

Options:
A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.
C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.
D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Answer: C

Explanation:

- A: Incorrect. Long polling reduces empty responses, not duplicates.

- B: Incorrect. FIFO is not necessary; visibility timeout handles retries.

- C: Correct. Longer visibility timeout prevents reprocessing before Lambda finishes.

- D: Incorrect. Premature delete risks message loss on failure.

Question 599:
A company is implementing a shared storage solution for a gaming application that is hosted in an on-premises data center. The company needs the ability to use Lustre clients to access data. The solution must be fully managed. Which solution meets these requirements?

Options:
A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Answer: D

Explanation:

- A: Incorrect. File Gateway does not support Lustre protocol.

- B: Incorrect. Windows file share is SMB, not Lustre.

- C: Incorrect. EFS is NFS, not Lustre.

- D: Correct. FSx for Lustre provides managed Lustre storage.

Question 600:
A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the certificates as needed. Control access to the data by using fine-grained IAM access.
B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.
C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.
D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

Answer: C

Explanation:

- A: Incorrect. Manual certificate updates add operational overhead.

- B: Incorrect. Custom Lambda crypto adds unnecessary complexity.

- C: Correct. KMS provides secure encryption, and S3 provides durable, HA storage.

- D: Incorrect. EBS is less durable and not suited for sharing certificates.

Question 601:

A financial company needs to handle highly sensitive data. The company will store the data in an Amazon S3 bucket. The company needs to ensure that the data is encrypted in transit and at rest. The company must manage the encryption keys outside the AWS Cloud. Which solution will meet these requirements?

Options:

A.Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key.

B.Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key.

C.Encrypt the data in the S3 bucket with the default server-side encryption (SSE).

D.Encrypt the data at the company's data center before storing the data in the S3 bucket.

Answer: D

Explanation:

- D is correct because client-side encryption before uploading ensures encryption keys are managed entirely outside AWS.

- A is wrong because customer managed CMKs are still within AWS KMS.

- B is wrong because AWS managed CMKs are controlled by AWS, not outside AWS.

- C is wrong because default SSE uses AWS-owned keys.

Question 602:

A company wants to run its payment application on AWS. The application receives payment notifications from mobile devices. Payment notifications require a basic validation before they are sent for further processing. The backend processing application is long running and requires compute and memory to be adjusted. The company does not want to manage the infrastructure. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A.Create an Amazon Simple Queue Service (Amazon SQS) queue. Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices. Configure the rule to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere. Create a standalone cluster.

B.Create an Amazon API Gateway API. Integrate the API with an AWS Step Functions state machine to receive payment notifications from mobile devices. Invoke the state machine to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure an EKS cluster with self-managed nodes.

C.Create an Amazon Simple Queue Service (Amazon SQS) queue. Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices. Configure the rule to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon EC2 Spot Instances. Configure a Spot Fleet with a default allocation strategy.

D.Create an Amazon API Gateway API. Integrate the API with AWS Lambda to receive payment notifications Question: 801 CertyIQ Question: 802 CertyIQ from mobile devices. Invoke a Lambda function to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS with an AWS Fargate launch type.

Answer: D

Explanation:

- D is correct because API Gateway + Lambda validates notifications, and ECS Fargate runs backend without managing servers.

- A is wrong because EKS Anywhere requires infrastructure management.

- B is wrong because self-managed EKS nodes add operational overhead.

- C is wrong because EC2 Spot introduces interruptions and management.

Question 603:
A solutions architect is designing a user authentication solution for a company. The solution must invoke twofactor authentication for users that log in from inconsistent geographical locations, IP addresses, or devices. The solution must also be able to scale up to accommodate millions of users. Which solution will meet these requirements?

Options:
A.Configure Amazon Cognito user pools for user authentication. Enable the risk-based adaptive authentication feature with multifactor authentication (MFA).
B.Configure Amazon Cognito identity pools for user authentication. Enable multi-factor authentication (MFA).
C.Configure AWS Identity and Access Management (IAM) users for user authentication. Attach an IAM policy that allows the AllowManageOwnUserMFA action.
D.Configure AWS IAM Identity Center (AWS Single Sign-On) authentication for user authentication. Configure the permission sets to require multi-factor authentication (MFA).

Answer: A

Explanation:

- A is correct because Cognito user pools support adaptive MFA and scale to millions of users.

- B is wrong because identity pools do not provide adaptive MFA features.

- C is wrong because IAM users are not designed for millions of external users.

- D is wrong because IAM Identity Center is for workforce SSO, not customer users.

Question 604:
A company has an Amazon S3 data lake. The company needs a solution that transforms the data from the data lake and loads the data into a data warehouse every day. The data warehouse must have massively parallel processing (MPP) capabilities. Data analysts then need to create and train machine learning (ML) models by using SQL commands on the data. The solution must use serverless AWS services wherever possible. Which solution will meet these requirements?

Options:
A.Run a daily Amazon EMR job to transform the data and load the data into Amazon Redshift. Use Amazon Redshift ML to create and train the ML models.
B.Run a daily Amazon EMR job to transform the data and load the data into Amazon Aurora Serverless. Use Amazon Aurora ML to create and train the ML models.
C.Run a daily AWS Glue job to transform the data and load the data into Amazon Redshift Serverless. Use Amazon Redshift ML to create and train the ML models.
D.Run a daily AWS Glue job to transform the data and load the data into Amazon Athena tables. Use Amazon Athena ML to create and train the ML models.

Answer: C

Explanation:

- C is correct because Glue is serverless for ETL, Redshift Serverless provides MPP and ML via Redshift ML.

- A is wrong because EMR adds operational overhead.

- B is wrong because Aurora does not provide MPP.

- D is wrong because Athena is not a warehouse and has limited ML support.

Question 605:
A company runs containers in a Kubernetes environment in the company's local data center. The company wants to use Amazon Elastic Kubernetes Service (Amazon EKS) and other AWS managed services. Data must remain locally in the company's data center and cannot be stored in any remote site or cloud to maintain compliance. Which solution will meet these requirements?

Options:
A.Deploy AWS Local Zones in the company's data center.
B.Use an AWS Snowmobile in the company's data center.
C.Install an AWS Outposts rack in the company's data center.
D.Install an AWS Snowball Edge Storage Optimized node in the data center.

Answer: C
Explanation:

- C is correct because Outposts brings AWS managed services like EKS into the data center.

- A is wrong because Local Zones are AWS-managed infrastructure, not in customer data centers.

- B is wrong because Snowmobile is only for large one-time data transfers.

- D is wrong because Snowball Edge is temporary edge compute, not full EKS integration.

Question 606:
A social media company has workloads that collect and process data. The workloads store the data in on-premises NFS storage. The data store cannot scale fast enough to meet the company's expanding business needs. The company wants to migrate the current data store to AWS. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Set up an AWS Storage Gateway Volume Gateway. Use an Amazon S3 Lifecycle policy to transition the data to the appropriate storage class.
B.Set up an AWS Storage Gateway Amazon S3 File Gateway. Use an Amazon S3 Lifecycle policy to transition the data to the appropriate storage class.
C.Use the Amazon Elastic File System (Amazon EFS) Standard-Infrequent Access (Standard-IA) storage class. Activate the infrequent access lifecycle policy.
D.Use the Amazon Elastic File System (Amazon EFS) One Zone-Infrequent Access (One Zone-IA) storage class. Activate the infrequent access lifecycle policy.
Answer: B

Explanation:

- B is correct because S3 File Gateway provides NFS interface backed by scalable S3 with lifecycle policies.

- A is wrong because Volume Gateway is block storage, not NFS-compatible.

- C is wrong because EFS is costlier than File Gateway for migration.

- D is wrong because One Zone-IA lacks multi-AZ resilience.

Question 607:
A company uses high concurrency AWS Lambda functions to process a constantly increasing number of messages in a message queue during marketing events. The Lambda functions use CPU intensive code to process the messages. The company wants to reduce the compute costs and to maintain service latency for its customers. Which solution will meet these requirements?
Options:
A.Configure reserved concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.
B.Configure reserved concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.
C.Configure provisioned concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.
D.Configure provisioned concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.
Answer: D
Explanation:

- D is correct because provisioned concurrency reduces cold starts and higher memory increases CPU, lowering execution time and cost.

- A is wrong because reducing memory reduces CPU, worsening performance.

- B is wrong because reserved concurrency only sets limits, doesn't solve latency.

- C is wrong because decreasing memory reduces CPU power for intensive tasks.

Question 608:
A company runs its workloads on Amazon Elastic Container Service (Amazon ECS). The container images that the ECS task definition uses need to be scanned for Common Vulnerabilities and Exposures (CVEs). New container images that are created also need to be scanned. Which solution will meet these requirements with the FEWEST changes to the workloads?

Options:
A.Use Amazon Elastic Container Registry (Amazon ECR) as a private image repository to store the container images. Specify scan on push filters for the ECR basic scan.

B.Store the container images in an Amazon S3 bucket. Use Amazon Macie to scan the images. Use an S3 Event Notification to initiate a Macie scan for every event with an s3:ObjectCreated:Put event type.

C.Deploy the workloads to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Container Registry (Amazon ECR) as a private image repository. Specify scan on push filters for the ECR enhanced scan.

D.Store the container images in an Amazon S3 bucket that has versioning enabled. Configure an S3 Event Notification for s3:ObjectCreated:* events to invoke an AWS Lambda function. Configure the Lambda function to initiate an Amazon Inspector scan.

Answer: A
Explanation:

- A is correct because ECS integrates natively with ECR and supports vulnerability scanning on push with minimal changes.

- B is wrong because Macie scans for sensitive data, not CVEs.

- C is wrong because migrating to EKS is unnecessary and adds overhead.

- D is wrong because Inspector is not used this way and adds complexity.

Question 609:
A company uses an AWS Batch job to run its end-of-day sales process. The company needs a serverless solution that will invoke a third-party reporting application when the AWS Batch job is successful. The reporting application has an HTTP API interface that uses username and password authentication. Which solution will meet these requirements?

Options:
A.Configure an Amazon EventBridge rule to match incoming AWS Batch job SUCCEEDED events. Configure the third-party API as an EventBridge API destination with a username and password. Set the API destination as the EventBridge rule target.

B.Configure Amazon EventBridge Scheduler to match incoming AWS Batch job SUCCEEDED events. Configure an AWS Lambda function to invoke the third-party API by using a username and password. Set the Lambda function as the EventBridge rule target.

C.Configure an AWS Batch job to publish job SUCCEEDED events to an Amazon API Gateway REST API. Configure an HTTP proxy integration on the API Gateway REST API to invoke the third-party API by using a username and password.

D.Configure an AWS Batch job to publish job SUCCEEDED events to an Amazon API Gateway REST API. Configure a proxy integration on the API Gateway REST API to an AWS Lambda function. Configure the Lambda function to invoke the third-party API by using a username and password.

Answer: B
Explanation:

- B is correct because EventBridge Scheduler and Lambda provide a serverless, simple solution for invoking APIs with credentials.

- A is wrong because EventBridge API destinations require more configuration and management.

- C is wrong because publishing directly to API Gateway adds complexity.

- D is wrong because it introduces unnecessary steps with API Gateway + Lambda.

Question 610:
A company collects and processes data from a vendor. The vendor stores its data in an Amazon RDS for MySQL database in the vendor's own AWS account. The company's VPC does not have an internet gateway, an AWS Direct Connect connection, or an AWS Site-to-Site VPN connection. The company needs to access the data that is in the vendor database. Which solution will meet this requirement?
Options:
A.Instruct the vendor to sign up for the AWS Hosted Connection Direct Connect Program. Use VPC peering to connect the company's VPC and the vendor's VPC.
B.Configure a client VPN connection between the company's VPC and the vendor's VPC. Use VPC peering to connect the company's VPC and the vendor's VPC.
C.Instruct the vendor to create a Network Load Balancer (NLB). Place the NLB in front of the Amazon RDS for MySQL database. Use AWS PrivateLink to integrate the company's VPC and the vendor's VPC.
D.Use AWS Transit Gateway to integrate the company's VPC and the vendor's VPC. Use VPC peering to connect the company's VPC and the vendor's VPC.
Answer: C
Explanation:

- C is correct because PrivateLink with NLB allows private access to the RDS database without internet.

- A is wrong because Direct Connect requires a physical connection.

- B is wrong because VPN introduces dependency on internet connectivity.

- D is wrong because Transit Gateway still needs internet or DX/VPN.

Question 611:
A company wants to set up Amazon Managed Grafana as its visualization tool. The company wants to visualize data from its Amazon RDS database as one data source. The company needs a secure solution that will not expose the data over the internet. Which solution will meet these requirements?
Options:
A.Create an Amazon Managed Grafana workspace without a VPC. Create a public endpoint for the RDS database. Configure the public endpoint as a data source in Amazon Managed Grafana.
B.Create an Amazon Managed Grafana workspace in a VPC. Create a private endpoint for the RDS database. Configure the private endpoint as a data source in Amazon Managed Grafana.
C.Create an Amazon Managed Grafana workspace without a VPCreate an AWS PrivateLink endpoint to establish a connection between Amazon Managed Grafana and Amazon RDS. Set up Amazon RDS as a data source in Amazon Managed Grafana.
D.Create an Amazon Managed Grafana workspace in a VPC. Create a public endpoint for the RDS database. Configure the public endpoint as a data source in Amazon Managed Grafana.
Answer: C

Explanation:

- C is correct because PrivateLink ensures secure connectivity between Grafana and RDS without exposing traffic to the internet.

- A is wrong because using a public endpoint exposes the database.

- B is wrong because a private endpoint works only if Grafana runs inside the same VPC.

- D is wrong because using a public endpoint is not secure.

Question 612:

A company hosts a data lake on Amazon S3. The data lake ingests data in Apache Parquet format from various data sources. The company uses multiple transformation steps to prepare the ingested data. The steps include filtering of anomalies, normalizing of data to standard date and time values, and generation of aggregates for analyses. The company must store the transformed data in S3 buckets that data analysts access. The company needs a prebuilt solution for data transformation that does not require code. The solution must provide data lineage and data profiling. The company needs to share the data transformation steps with employees throughout the company. Which solution will meet these requirements?

Options:

A.Configure an AWS Glue Studio visual canvas to transform the data. Share the transformation steps with employees by using AWS Glue jobs.

B.Configure Amazon EMR Serverless to transform the data. Share the transformation steps with employees by using EMR Serverless jobs.

C.Configure AWS Glue DataBrew to transform the data. Share the transformation steps with employees by using DataBrew recipes.

D.Create Amazon Athena tables for the data. Write Athena SQL queries to transform the data. Share the Athena SQL queries with employees.

Answer: C

Explanation:

- C is correct because Glue DataBrew is a no-code transformation tool with data lineage and profiling that can share recipes.

- A is wrong because Glue Studio requires more technical setup for profiling.

- B is wrong because EMR is code-based and adds operational overhead.

- D is wrong because Athena SQL queries do not provide profiling or lineage.

Question 613:
A solutions architect runs a web application on multiple Amazon EC2 instances that are in individual target groups behind an Application Load Balancer (ALB). Users can reach the application through a public website. The solutions architect wants to allow engineers to use a development version of the website to access one specific development EC2 instance to test new features for the application. The solutions architect wants to use an Amazon Route 53 hosted zone to give the engineers access to the development instance. The solution must automatically route to the development instance even if the development instance is replaced. Which solution will meet these requirements?

Options:
A.Create an A Record for the development website that has the value set to the ALB. Create a listener rule on the ALB that forwards requests for the development website to the target group that contains the development instance.
B.Recreate the development instance with a public IP address. Create an A Record for the development website that has the value set to the public IP address of the development instance.
C.Create an A Record for the development website that has the value set to the ALB. Create a listener rule on the ALB to redirect requests for the development website to the public IP address of the development instance.
D.Place all the instances in the same target group. Create an A Record for the development website. Set the value to the ALB. Create a listener rule on the ALB that forwards requests for the development website to the target group.

Answer: A
Explanation:

- A is correct because an ALB listener rule forwarding to a dev target group ensures routing even if instance changes.

- B is wrong because a public IP breaks when the instance is replaced.

- C is wrong because redirecting to an IP is not supported in ALB rules.

- D is wrong because mixing all instances into one target group removes separation.

Question 614:
A company runs a container application on a Kubernetes cluster in the company's data center. The application uses Advanced Message Queuing Protocol (AMQP) to communicate with a message queue. The data center cannot scale fast enough to meet the company's expanding business needs. The company wants to migrate the workloads to AWS. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Migrate the container application to Amazon Elastic Container Service (Amazon ECS). Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.
B.Migrate the container application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon MQ to retrieve the messages.
C.Use highly available Amazon EC2 instances to run the application. Use Amazon MQ to retrieve the messages.
D.Use AWS Lambda functions to run the application. Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.

Answer: B
Explanation:

- B is correct because EKS provides managed Kubernetes and Amazon MQ supports AMQP natively.

- A is wrong because SQS does not support AMQP.

- C is wrong because EC2 requires manual management and scaling.

- D is wrong because Lambda is not suitable for long-running container workloads.

Question 615:
An online gaming company hosts its platform on Amazon EC2 instances behind Network Load Balancers (NLBs) across multiple AWS Regions. The NLBs can route requests to targets over the internet. The company wants to improve the customer playing experience by reducing end-to-end load time for its global customer base. Which solution will meet these requirements?
Options:
A.Create Application Load Balancers (ALBs) in each Region to replace the existing NLBs. Register the existing EC2 instances as targets for the ALBs in each Region.
B.Configure Amazon Route 53 to route equally weighted traffic to the NLBs in each Region.
C.Create additional NLBs and EC2 instances in other Regions where the company has large customer bases.
D.Create a standard accelerator in AWS Global Accelerator. Configure the existing NLBs as target endpoints.
Answer: D
Explanation:

- D is correct because Global Accelerator reduces latency by routing traffic via AWS global edge network.

- A is wrong because ALBs don't reduce latency across Regions.

- B is wrong because Route 53 routing does not accelerate network traffic.

- C is wrong because more NLBs still rely on internet routing.

Question 616:
A company has an on-premises application that uses SFTP to collect financial data from multiple vendors. The company is migrating to the AWS Cloud. The company has created an application that uses Amazon S3 APIs to upload files from vendors. Some vendors run their systems on legacy applications that do not support S3 APIs. The vendors want to continue to use SFTP-based applications to upload data. The company wants to use managed services for the needs of the vendors that use legacy applications. Which solution will meet these requirements with the LEAST operational overhead?
Options:
A.Create an AWS Database Migration Service (AWS DMS) instance to replicate data from the storage of the vendors that use legacy applications to Amazon S3. Provide the vendors with the credentials to access the AWS DMS instance.
B.Create an AWS Transfer Family endpoint for vendors that use legacy applications.
C.Configure an Amazon EC2 instance to run an SFTP server. Instruct the vendors that use legacy applications to use the SFTP server to upload data.
D.Configure an Amazon S3 File Gateway for vendors that use legacy applications to upload files to an SMB file share.
Answer: B
Explanation:

- B is correct because AWS Transfer Family provides a fully managed SFTP solution integrated with S3.

- A is wrong because DMS is for databases, not file transfers.

- C is wrong because running SFTP on EC2 requires management.

- D is wrong because File Gateway supports NFS/SMB, not SFTP.

Question 617:

A marketing team wants to build a campaign for an upcoming multi-sport event. The team has news reports from the past five years in PDF format. The team needs a solution to extract insights about the content and the sentiment of the news reports. The solution must use Amazon Textract to process the news reports. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A.Provide the extracted insights to Amazon Athena for analysis. Store the extracted insights and analysis in an Amazon S3 bucket.

B.Store the extracted insights in an Amazon DynamoDB table. Use Amazon SageMaker to build a sentiment model.

C.Provide the extracted insights to Amazon Comprehend for analysis. Save the analysis to an Amazon S3 bucket.

D.Store the extracted insights in an Amazon S3 bucket. Use Amazon QuickSight to visualize and analyze the data.

Answer: C

Explanation:

- C is correct because Textract extracts text and Comprehend analyzes sentiment with minimal management.

- A is wrong because Athena is for SQL querying, not NLP sentiment analysis.

- B is wrong because SageMaker requires building and training custom models.

- D is wrong because QuickSight is visualization only, not NLP.

Question 618:

A company's application runs on Amazon EC2 instances that are in multiple Availability Zones. The application needs to ingest real-time data from third-party applications. The company needs a data ingestion solution that places the ingested raw data in an Amazon S3 bucket. Which solution will meet these requirements?

Options:

A.Create Amazon Kinesis data streams for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume the Kinesis data streams. Specify the S3 bucket as the destination of the delivery streams.

B.Create database migration tasks in AWS Database Migration Service (AWS DMS). Specify replication instances of the EC2 instances as the source endpoints. Specify the S3 bucket as the target endpoint. Set the migration type to migrate existing data and replicate ongoing changes.

C.Create and configure AWS DataSync agents on the EC2 instances. Configure DataSync tasks to transfer data Question: 817 CertyIQ Question: 818 CertyIQ from the EC2 instances to the S3 bucket.

D.Create an AWS Direct Connect connection to the application for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume direct PUT operations from the application. Specify the S3 bucket as the destination of the delivery streams.

Answer: A
Explanation:

- A is correct because Kinesis + Firehose provides scalable real-time ingestion directly into S3.

- B is wrong because DMS is for databases, not general data streams.

- C is wrong because DataSync is for batch transfers, not streaming.

- D is wrong because Direct Connect is unnecessary and adds cost.

Question 619:
A company's application is receiving data from multiple data sources. The size of the data varies and is expected to increase over time. The current maximum size is 700 KB. The data volume and data size continue to grow as more data sources are added. The company decides to use Amazon DynamoDB as the primary database for the application. A solutions architect needs to identify a solution that handles the large data sizes. Which solution will meet these requirements in the MOST operationally efficient way?
Options:
A.Create an AWS Lambda function to filter the data that exceeds DynamoDB item size limits. Store the larger data in an Amazon DocumentDB (with MongoDB compatibility) database.
B.Store the large data as objects in an Amazon S3 bucket. In a DynamoDB table, create an item that has an attribute that points to the S3 URL of the data.
C.Split all incoming large data into a collection of items that have the same partition key. Write the data to a DynamoDB table in a single operation by using the BatchWriteItem API operation.
D.Create an AWS Lambda function that uses gzip compression to compress the large objects as they are written to a DynamoDB table.
Answer: B
Explanation:

- B is correct because storing large objects in S3 with references in DynamoDB is efficient and scalable.

- A is wrong because DocumentDB adds complexity and cost.

- C is wrong because splitting items increases complexity and breaks atomicity.

- D is wrong because compression doesn't bypass the 400 KB DynamoDB item limit.

Question 620:
A company is migrating a legacy application from an on-premises data center to AWS. The application relies on hundreds of cron jobs that run between 1 and 20 minutes on different recurring schedules throughout the day. The company wants a solution to schedule and run the cron jobs on AWS with minimal refactoring. The solution must support running the cron jobs in response to an event in the future. Which solution will meet these requirements?
Options:
A.Create a container image for the cron jobs. Use Amazon EventBridge Scheduler to create a recurring schedule. Run the cron job tasks as AWS Lambda functions.
B.Create a container image for the cron jobs. Use AWS Batch on Amazon Elastic Container Service (Amazon ECS) with a scheduling policy to run the cron jobs.
C.Create a container image for the cron jobs. Use Amazon EventBridge Scheduler to create a recurring schedule. Run the cron job tasks on AWS Fargate.
D.Create a container image for the cron jobs. Create a workflow in AWS Step Functions that uses a Wait state to run the cron jobs at a specified time. Use the RunTask action to run the cron job tasks on AWS Fargate.

Answer: C

Explanation:

- C is correct because EventBridge Scheduler + Fargate supports container cron jobs without managing servers.

- A is wrong because Lambda has runtime limits, unsuitable for 20-minute jobs.

- B is wrong because AWS Batch is designed for batch processing, not cron jobs.

- D is wrong because Step Functions with Wait states is more complex.

Question 621:
A company uses Salesforce. The company needs to load existing data and ongoing data changes from Salesforce to Amazon Redshift for analysis. The company does not want the data to travel over the public internet. Which solution will meet these requirements with the LEAST development effort?

Options:
A.Establish a VPN connection from the VPC to Salesforce. Use AWS Glue DataBrew to transfer data.
B.Establish an AWS Direct Connect connection from the VPC to Salesforce. Use AWS Glue DataBrew to transfer data.
C.Create an AWS PrivateLink connection in the VPC to Salesforce. Use Amazon AppFlow to transfer data.
D.Create a VPC peering connection to Salesforce. Use Amazon AppFlow to transfer data.

Answer: C

Explanation:

- C is correct because AppFlow integrates natively with Salesforce and PrivateLink keeps traffic private.

- A is wrong because VPN still traverses the public internet.

- B is wrong because Salesforce doesn't support DX directly.

- D is wrong because VPC peering is not possible with Salesforce.

Question 622:
A company recently migrated its application to AWS. The application runs on Amazon EC2 Linux instances in an Auto Scaling group across multiple Availability Zones. The application stores data in an Amazon Elastic File System (Amazon EFS) file system that uses EFS Standard-Infrequent Access storage. The application indexes the company's files. The index is stored in an Amazon RDS database. The company needs to optimize storage costs with some application and services changes. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create an Amazon S3 bucket that uses an Intelligent-Tiering lifecycle policy. Copy all files to the S3 bucket. Update the application to use Amazon S3 API to store and retrieve files.
B.Deploy Amazon FSx for Windows File Server file shares. Update the application to use CIFS protocol to store and retrieve files.
C.Deploy Amazon FSx for OpenZFS file system shares. Update the application to use the new mount point to store and retrieve files.
D.Create an Amazon S3 bucket that uses S3 Glacier Flexible Retrieval. Copy all files to the S3 bucket. Update the application to use Amazon S3 API to store and retrieve files as standard retrievals.

Answer: A
Explanation:

- A is correct because S3 Intelligent-Tiering optimizes storage costs automatically with minimal changes.

- B is wrong because FSx for Windows is expensive and not needed.

- C is wrong because FSx for OpenZFS doesn't provide cost savings for this workload.

- D is wrong because Glacier adds retrieval delays unsuitable for app access.

Question 623:
A robotics company is designing a solution for medical surgery. The robots will use advanced sensors, cameras, and AI algorithms to perceive their environment and to complete surgeries. The company needs a public load balancer in the AWS Cloud that will ensure seamless communication with backend services. The load balancer must be capable of routing traffic based on the query strings to different target groups. The traffic must also be encrypted. Which solution will meet these requirements?
Options:
A.Use a Network Load Balancer with a certificate attached from AWS Certificate Manager (ACM). Use query parameter-based routing.
B.Use a Gateway Load Balancer. Import a generated certificate in AWS Identity and Access Management (IAM). Attach the certificate to the load balancer. Use HTTP path-based routing.
C.Use an Application Load Balancer with a certificate attached from AWS Certificate Manager (ACM). Use query parameter-based routing.
D.Use a Network Load Balancer. Import a generated certificate in AWS Identity and Access Management (IAM). Attach the certificate to the load balancer. Use query parameter-based routing.
Answer: C
Explanation:

- C is correct because ALB supports query string–based routing and SSL with ACM.

- A is wrong because NLB doesn't support query-based routing.

- B is wrong because Gateway Load Balancer is for appliances, not query routing.

- D is wrong because NLB cannot do query parameter routing.

Question 624:
A company has an application that runs on a single Amazon EC2 instance. The application uses a MySQL database that runs on the same EC2 instance. The company needs a highly available and automatically scalable solution to handle increased traffic. Which solution will meet these requirements?
Options:
A.Deploy the application to EC2 instances that run in an Auto Scaling group behind an Application Load Balancer. Create an Amazon Redshift cluster that has multiple MySQL-compatible nodes.
B.Deploy the application to EC2 instances that are configured as a target group behind an Application Load Balancer. Create an Amazon RDS for MySQL cluster that has multiple instances.
C.Deploy the application to EC2 instances that run in an Auto Scaling group behind an Application Load Balancer. Create an Amazon Aurora Serverless MySQL cluster for the database layer.

D.Deploy the application to EC2 instances that are configured as a target group behind an Application Load Balancer. Create an Amazon ElastiCache for Redis cluster that uses the MySQL connector.

Answer: C

Explanation:

- C is correct because Aurora Serverless provides auto scaling and high availability for MySQL workloads.

- A is wrong because Redshift is a data warehouse, not a transactional DB.

- B is wrong because RDS provides HA but not true auto scaling.

- D is wrong because Redis is a cache, not a relational DB replacement.

Question 625:
A company is planning to migrate data to an Amazon S3 bucket. The data must be encrypted at rest within the S3 bucket. The encryption key must be rotated automatically every year. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Migrate the data to the S3 bucket. Use server-side encryption with Amazon S3 managed keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
B.Create an AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Migrate the data to the S3 bucket.
C.Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Migrate the data to the S3 bucket. Manually rotate the KMS key every year.
D.Use customer key material to encrypt the data. Migrate the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Answer: A

Explanation:

- A is correct because SSE-S3 manages encryption and automatically rotates keys yearly without effort.

- B is wrong because KMS CMKs require more setup and cost.

- C is wrong because manual rotation increases operational overhead.

- D is wrong because customer key material rotation is not automatic.

Question 626:
AWS. The company deploys the applications in multiple AWS accounts. The company uses AWS Organizations to manage the accounts centrally. The company's security team needs a single sign-on solution across all the company's AWS accounts. The company must continue to manage users and groups that are in the on-premises Active Directory. Which solution will meet these requirements?

Options:
A.Create an Enterprise Edition Active Directory in AWS Directory Service for Microsoft Active Directory. Question: 824 CertyIQ Question: 825 CertyIQ Question: 826 CertyIQ Configure the Active Directory to be the identity source for AWS IAM Identity Center.
B.Enable AWS IAM Identity Center. Configure a two-way forest trust relationship to connect the company's self-managed Active Directory with IAM Identity Center by using AWS Directory Service for Microsoft Active Directory.
C.Use AWS Directory Service and create a two-way trust relationship with the company's self-managed Active Directory.
D.Deploy an identity provider (IdP) on Amazon EC2. Link the IdP as an identity source within AWS IAM Identity Center.

Answer: B
Explanation:

- B is correct because IAM Identity Center supports integration with self-managed AD via Directory Service and trust relationship.

- A is wrong because creating a new AWS-managed AD doesn't use the existing on-premises AD.

- C is wrong because Directory Service alone doesn't provide SSO across Organizations accounts.

- D is wrong because running IdP on EC2 increases overhead unnecessarily.

Question 627:
A company is planning to deploy its application on an Amazon Aurora PostgreSQL Serverless v2 cluster. The application will receive large amounts of traffic. The company wants to optimize the storage performance of the cluster as the load on the application increases. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Configure the cluster to use the Aurora Standard storage configuration.
B.Configure the cluster storage type as Provisioned IOPS.
C.Configure the cluster storage type as General Purpose.
D.Configure the cluster to use the Aurora I/O-Optimized storage configuration.

Answer: C
Explanation:

- C is correct because General Purpose storage balances cost and performance efficiently for scaling workloads.

- A is wrong because Aurora Standard storage configuration is outdated.

- B is wrong because Provisioned IOPS is more expensive and unnecessary here.

- D is wrong because I/O-Optimized is higher cost and used for intensive I/O workloads.

Question 628:

A financial services company that runs on AWS has designed its security controls to meet industry standards. The industry standards include the National Institute of Standards and Technology (NIST) and the Payment Card Industry Data Security Standard (PCI DSS). The company's third-party auditors need proof that the designed controls have been implemented and are functioning correctly. The company has hundreds of AWS accounts in a single organization in AWS Organizations. The company needs to monitor the current state of the controls across accounts. Which solution will meet these requirements?

Options:

A.Designate one account as the Amazon Inspector delegated administrator account from the Organizations management account. Integrate Inspector with Organizations to discover and scan resources across all AWS accounts. Enable Inspector industry standards for NIST and PCI DSS.

B.Designate one account as the Amazon GuardDuty delegated administrator account from the Organizations management account. In the designated GuardDuty administrator account, enable GuardDuty to protect all member accounts. Enable GuardDuty industry standards for NIST and PCI DSS.

C.Configure an AWS CloudTrail organization trail in the Organizations management account. Designate one account as the compliance account. Enable CloudTrail security standards for NIST and PCI DSS in the compliance account.

D.Designate one account as the AWS Security Hub delegated administrator account from the Organizations management account. In the designated Security Hub administrator account, enable Security Hub for all member accounts. Enable Security Hub standards for NIST and PCI DSS.

Answer: D

Explanation:

- D is correct because Security Hub provides compliance checks against NIST and PCI DSS standards across accounts.

- A is wrong because Inspector scans vulnerabilities, not compliance standards.

- B is wrong because GuardDuty focuses on threat detection, not compliance reporting.

- C is wrong because CloudTrail is logging, not compliance enforcement.

Question 629:

A company uses an Amazon S3 bucket as its data lake storage platform. The S3 bucket contains a massive amount of data that is accessed randomly by multiple teams and hundreds of applications. The company wants to reduce the S3 storage costs and provide immediate availability for frequently accessed objects. What is the MOST operationally efficient solution that meets these requirements?

Options:

A.Create an S3 Lifecycle rule to transition objects to the S3 Intelligent-Tiering storage class.

B.Store objects in Amazon S3 Glacier. Use S3 Select to provide applications with access to the data.

C.Use data from S3 storage class analysis to create S3 Lifecycle rules to automatically transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class.

D.Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an AWS Lambda function to transition objects to the S3 Standard storage class when they are accessed by an application.

Answer: A
Explanation:

- A is correct because Intelligent-Tiering automatically optimizes storage class with no performance impact.

- B is wrong because Glacier does not provide immediate access.

- C is wrong because S3 Standard-IA charges retrieval costs and lacks automation.

- D is wrong because manually triggering Lambda adds operational overhead.

Question 630:
A company has 5 TB of datasets. The datasets consist of 1 million user profiles and 10 million connections. The user profiles have connections as many-to-many relationships. The company needs a performance efficient way to find mutual connections up to five levels. Which solution will meet these requirements?
Options:
A.Use an Amazon S3 bucket to store the datasets. Use Amazon Athena to perform SQL JOIN queries to find connections.
B.Use Amazon Neptune to store the datasets with edges and vertices. Query the data to find connections.
C.Use an Amazon S3 bucket to store the datasets. Use Amazon QuickSight to visualize connections.
D.Use Amazon RDS to store the datasets with multiple tables. Perform SQL JOIN queries to find connections.
Answer: B
Explanation:

- B is correct because Neptune is optimized for graph queries like multi-level relationships.

- A is wrong because Athena SQL JOINs are inefficient for deep graph queries.

- C is wrong because QuickSight is visualization only.

- D is wrong because relational joins for 5-level connections are slow and costly.

Question 631:
A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly. What is the MOST cost-effective method to establish this type of connection?
Options:
A.Implement a client VPN.
B.Implement AWS Direct Connect.
C.Implement a bastion host on Amazon EC2.
D.Implement an AWS Site-to-Site VPN connection.
Answer: D

Explanation:

- D is correct because Site-to-Site VPN provides secure, quick setup with low bandwidth needs.

- A is wrong because client VPN is for user devices, not site-to-site.

- B is wrong because Direct Connect is costly and not needed for low traffic.

- C is wrong because a bastion host is not a secure site-to-site tunnel.

Question 632:
A company has an on-premises SFTP file transfer solution. The company is migrating to the AWS Cloud to scale the file transfer solution and to optimize costs by using Amazon S3. The company's employees will use their credentials for the on-premises Microsoft Active Directory (AD) to access the new solution. The company wants to keep the current authentication and file access mechanisms. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Configure an S3 File Gateway. Create SMB file shares on the file gateway that use the existing Active Directory to authenticate.
B.Configure an Auto Scaling group with Amazon EC2 instances to run an SFTP solution. Configure the group to scale up at 60% CPU utilization.
C.Create an AWS Transfer Family server with SFTP endpoints. Choose the AWS Directory Service option as the identity provider. Use AD Connector to connect the on-premises Active Directory.
D.Create an AWS Transfer Family SFTP endpoint. Configure the endpoint to use the AWS Directory Service option as the identity provider to connect to the existing Active Directory.

Answer: C

Explanation:

- C is correct because Transfer Family integrates with S3 and AD Connector for seamless authentication.

- A is wrong because File Gateway provides SMB/NFS, not SFTP.

- B is wrong because managing EC2-based SFTP adds overhead.

- D is wrong because Transfer Family requires AD Connector for integration.

Question 633:

A company is designing an event-driven order processing system. Each order requires multiple validation steps after the order is created. An idempotent AWS Lambda function performs each validation step. Each validation step is independent from the other validation steps. Individual validation steps need only a subset of the order event information. The company wants to ensure that each validation step Lambda function has access to only the information from the order event that the function requires. The components of the order processing system should be loosely coupled to accommodate future business changes. Which solution will meet these requirements?

Options:

A.Create an Amazon Simple Queue Service (Amazon SQS) queue for each validation step. Create a new Lambda function to transform the order data to the format that each validation step requires and to publish the messages to the appropriate SQS queues. Subscribe each validation step Lambda function to its corresponding SQS queue.

B.Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the validation step Lambda functions to the SNS topic. Use message body filtering to send only the required data to each subscribed Lambda function.

C.Create an Amazon EventBridge event bus. Create an event rule for each validation step. Configure the input transformer to send only the required data to each target validation step Lambda function.

D.Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a new Lambda function to subscribe to the SQS queue and to transform the order data to the format that each validation step requires. Use the new Lambda function to perform synchronous invocations of the validation step Lambda functions in parallel on separate threads.

Answer: C

Explanation:

- C is correct because EventBridge rules with input transformers provide targeted, loosely coupled event routing.

- A is wrong because managing many SQS queues increases complexity.

- B is wrong because SNS message filtering is limited for complex transformations.

- D is wrong because synchronous invocation couples the workflow tightly.

Question 634:

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

Options:

A.Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.

B.Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.

C.Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.

D.Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: C

Explanation:

- C is correct because Aurora with read replicas offloads reporting queries, improving performance.

- A is wrong because refactoring to DynamoDB is unnecessary and costly.

- B is wrong because running DB on EC2 increases management effort.

- D is wrong because backup instances are not intended for reporting.

Question 635:
A company is expanding a secure on-premises network to the AWS Cloud by using an AWS Direct Connect connection. The on-premises network has no direct internet access. An application that runs on the on-premises network needs to use an Amazon S3 bucket. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create a public virtual interface (VIF). Route the AWS traffic over the public VIF.
B.Create a VPC and a NAT gateway. Route the AWS traffic from the on-premises network to the NAT gateway.
C.Create a VPC and an Amazon S3 interface endpoint. Route the AWS traffic from the on-premises network to the S3 interface endpoint.
D.Create a VPC peering connection between the on-premises network and Direct Connect. Route the AWS traffic over the peering connection.

Answer: C

Explanation:

- C is correct because an S3 interface endpoint keeps traffic private without internet.

- A is wrong because a public VIF exposes traffic over internet paths.

- B is wrong because NAT adds unnecessary cost and complexity.

- D is wrong because VPC peering does not apply to Direct Connect.

Question 636:
A company serves its website by using an Auto Scaling group of Amazon EC2 instances in a single AWS Region. The website does not require a database. The company is expanding, and the company's engineering team deploys the website to a second Region. The company wants to distribute traffic across both Regions to accommodate growth and for disaster recovery purposes. The solution should not serve traffic from a Region in which the website is unhealthy. Which policy or resource should the company use to meet these requirements?

Options:
A.An Amazon Route 53 simple routing policy
B.An Amazon Route 53 multivalue answer routing policy
C.An Application Load Balancer in one Region with a target group that specifies the EC2 instance IDs from both Regions
D.An Application Load Balancer in one Region with a target group that specifies the IP addresses of the EC2 instances from both Regions

Answer: B

Explanation:

- B is correct because Route 53 multivalue routing supports health checks across Regions.

- A is wrong because simple routing doesn't support failover or health checks.

- C is wrong because ALB cannot span multiple Regions.

- D is wrong because ALB target groups don't support cross-Region IPs.

Question 637:
A company runs its applications on Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS). The EC2 instances run the most recent Amazon Linux release. The applications are experiencing availability issues when the company's employees store and retrieve files that are 25 GB or larger. The company needs a solution that does not require the company to transfer files between EC2 instances. The files must be available across many EC2 instances and across multiple Availability Zones. Which solution will meet these requirements?
Options:
A.Migrate all the files to an Amazon S3 bucket. Instruct the employees to access the files from the S3 bucket.
B.Take a snapshot of the existing EBS volume. Mount the snapshot as an EBS volume across the EC2 instances. Instruct the employees to access the files from the EC2 instances.
C.Mount an Amazon Elastic File System (Amazon EFS) file system across all the EC2 instances. Instruct the employees to access the files from the EC2 instances.
D.Create an Amazon Machine Image (AMI) from the EC2 instances. Configure new EC2 instances from the AMI that use an instance store volume. Instruct the employees to access the files from the EC2 instances.
Answer: C
Explanation:

- C is correct because EFS is scalable, multi-AZ, and supports concurrent access.

- A is wrong because S3 requires app changes to access files.

- B is wrong because snapshots are point-in-time copies, not shared storage.

- D is wrong because instance store is ephemeral and unsuitable.

Question 638:
A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest. Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?
Options:
A.Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
B.Deploy AWS CloudHSM, generate encryption keys, and use the keys to encrypt database volumes.
C.Configure SSL encryption using AWS Key Management Service (AWS KMS) keys to encrypt database volumes.
D.Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.
Answer: C

Explanation:

- C is correct because KMS-based SSL encryption provides compliance with minimal changes.

- A is wrong because ACM is for TLS/SSL certificates in transit, not at rest.

- B is wrong because CloudHSM adds unnecessary complexity.

- D is wrong because enabling EBS + RDS encryption requires reconfiguration of resources.

Question 639:
A company runs an AWS Lambda function in private subnets in a VPC. The subnets have a default route to the internet through an Amazon EC2 NAT instance. The Lambda function processes input data and saves its output as an object to Amazon S3. Intermittently, the Lambda function times out while trying to upload the object because of saturated traffic on the NAT instance's network. The company wants to access Amazon S3 without traversing the internet. Which solution will meet these requirements?
Options:
A.Replace the EC2 NAT instance with an AWS managed NAT gateway.
B.Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type.
C.Provision a gateway endpoint for Amazon S3 in the VPUpdate the route tables of the subnets accordingly.
D.Provision a transit gateway. Place transit gateway attachments in the private subnets where the Lambda function is running.
Answer: C
Explanation:

- C is correct because an S3 gateway endpoint enables private access without NAT or internet.

- A is wrong because NAT gateway still traverses the internet.

- B is wrong because larger NAT doesn't remove the internet dependency.

- D is wrong because a transit gateway is unnecessary for S3 access.

Question 640:
A news company that has reporters all over the world is hosting its broadcast system on AWS. The reporters send live broadcasts to the broadcast system. The reporters use software on their phones to send live streams through the Real Time Messaging Protocol (RTMP). A solutions architect must design a solution that gives the reporters the ability to send the highest quality streams. The solution must provide accelerated TCP connections back to the broadcast system. What should the solutions architect use to meet these requirements?
Options:
A.Amazon CloudFront
B.AWS Global Accelerator
C.AWS Client VPN
D.Amazon EC2 instances and AWS Elastic IP addresses
Answer: B

Explanation:

- B is correct because Global Accelerator accelerates TCP traffic over the AWS backbone.

- A is wrong because CloudFront is for content delivery, not input acceleration.

- C is wrong because Client VPN is for secure user access.

- D is wrong because EC2 with Elastic IP does not optimize TCP connections.

Question 641:
A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) to run its self-managed database. The company has 350 TB of data spread across all EBS volumes. The company takes daily EBS snapshots and keeps the snapshots for 1 month. The daily change rate is 5% of the EBS volumes. Because of new regulations, the company needs to keep the monthly snapshots for 7 years. The company needs to change its backup strategy to comply with the new regulations and to ensure that data is available with minimal administrative effort. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Keep the daily snapshot in the EBS snapshot standard tier for 1 month. Copy the monthly snapshot to Amazon S3 Glacier Deep Archive with a 7-year retention period.
B.Continue with the current EBS snapshot policy. Add a new policy to move the monthly snapshot to Amazon EBS Snapshots Archive with a 7-year retention period.
C.Keep the daily snapshot in the EBS snapshot standard tier for 1 month. Keep the monthly snapshot in the standard tier for 7 years. Use incremental snapshots.
D.Keep the daily snapshot in the EBS snapshot standard tier. Use EBS direct APIs to take snapshots of all the EBS volumes every month. Store the snapshots in an Amazon S3 bucket in the Infrequent Access tier for 7 years.
Answer: B
Explanation:

- B is correct because EBS Snapshots Archive is designed for long-term retention at lower cost.

- A is wrong because Glacier Deep Archive is not the native integration for EBS snapshots.

- C is wrong because keeping snapshots in standard tier for 7 years is expensive.

- D is wrong because exporting snapshots to S3 adds complexity.

Question 642:
A company runs an application on several Amazon EC2 instances that store persistent data on an Amazon Elastic File System (Amazon EFS) file system. The company needs to replicate the data to another AWS Region by using an AWS managed service solution. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Use the EFS-to-EFS backup solution to replicate the data to an EFS file system in another Region.
B.Run a nightly script to copy data from the EFS file system to an Amazon S3 bucket. Enable S3 Cross-Region Replication on the S3 bucket.
C.Create a VPC in another Region. Establish a cross-Region VPC peer. Run a nightly rsync to copy data from the original Region to the new Region.
D.Use AWS Backup to create a backup plan with a rule that takes a daily backup and replicates it to another Region. Assign the EFS file system resource to the backup plan.

Answer: A
Explanation:

- A is correct because EFS-to-EFS replication is fully managed and cost-effective.

- B is wrong because S3 replication introduces extra steps and complexity.

- C is wrong because manual rsync is not managed and adds overhead.

- D is wrong because AWS Backup is more expensive than direct EFS replication.

Question 643:
An ecommerce company is migrating its on-premises workload to the AWS Cloud. The workload currently consists of a web application and a backend Microsoft SQL database for storage. The company expects a high volume of customers during a promotional event. The new infrastructure in the AWS Cloud must be highly available and scalable. Which solution will meet these requirements with the LEAST administrative overhead?
Options:
A.Migrate the web application to two Amazon EC2 instances across two Availability Zones behind an Application Load Balancer. Migrate the database to Amazon RDS for Microsoft SQL Server with read replicas in both Availability Zones.
B.Migrate the web application to an Amazon EC2 instance that runs in an Auto Scaling group across two Availability Zones behind an Application Load Balancer. Migrate the database to two EC2 instances across separate AWS Regions with database replication.
C.Migrate the web application to Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones behind an Application Load Balancer. Migrate the database to Amazon RDS with Multi-AZ deployment.
D.Migrate the web application to three Amazon EC2 instances across three Availability Zones behind an Application Load Balancer. Migrate the database to three EC2 instances across three Availability Zones.
Answer: C
Explanation:

- C is correct because Auto Scaling + RDS Multi-AZ provides HA and scalability with minimal overhead.

- A is wrong because SQL Server read replicas are not widely supported.

- B is wrong because manual replication across Regions is complex.

- D is wrong because managing DBs on EC2 increases complexity.

Question 644:
A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS. The application development team does not have time to make the necessary code modifications to move the application to AWS. Which service should a solutions architect recommend to allow the application to copy files to AWS?
Options:
A.Amazon Elastic File System (Amazon EFS)
B.Amazon FSx for Windows File Server
C.AWS Snowball
D.AWS Storage Gateway

Answer: D

Explanation:

- D is correct because Storage Gateway provides SMB support and integrates with S3.

- A is wrong because EFS uses NFS, not SMB.

- B is wrong because FSx for Windows adds cost and overhead.

- C is wrong because Snowball is for bulk offline transfers.

Question 645:

A company has 15 employees. The company stores employee start dates in an Amazon DynamoDB table. The company wants to send an email message to each employee on the day of the employee's work anniversary. Which solution will meet these requirements with the MOST operational efficiency?

Options:

A.Create a script that scans the DynamoDB table and uses Amazon Simple Notification Service (Amazon SNS) to send email messages to employees when necessary. Use a cron job to run this script every day on an Amazon EC2 instance.

B.Create a script that scans the DynamoDB table and uses Amazon Simple Queue Service (Amazon SQS) to send email messages to employees when necessary. Use a cron job to run this script every day on an Amazon EC2 instance.

C.Create an AWS Lambda function that scans the DynamoDB table and uses Amazon Simple Notification Service (Amazon SNS) to send email messages to employees when necessary. Schedule this Lambda function to run every day.

D.Create an AWS Lambda function that scans the DynamoDB table and uses Amazon Simple Queue Service (Amazon SQS) to send email messages to employees when necessary. Schedule this Lambda function to run every day.

Answer: C

Explanation:

- C is correct because Lambda with SNS provides serverless, automated email sending with no servers.

- A is wrong because running scripts on EC2 adds management.

- B is wrong because SQS does not send emails directly.

- D is wrong because SQS is unnecessary for this workflow.

Question 646:

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users. Which solution will meet these requirements?

Options:

A.Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.

B.Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.

C.Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.

D.Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling:EC2_INSTANCE_LAUNCH events.
Answer: B
Explanation:

- B is correct because scheduled scaling ensures capacity is added before peak demand.

- A is wrong because scaling after CPU spikes is reactive, not proactive.

- C is wrong because manually changing min/max requires intervention.

- D is wrong because SNS notifications don't scale resources.

Question 647:
A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases. Which solution meets this requirement with the LEAST operational overhead?
Options:
A.Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.
B.Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.
C.Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.
D.Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the AWS KMS key.
Answer: A
Explanation:

- A is correct because Secrets Manager integrates with RDS and supports automatic rotation.

- B is wrong because Parameter Store does not support automatic DB password rotation.

- C is wrong because it requires custom rotation Lambda.

- D is wrong because KMS rotates encryption keys, not DB passwords.

Question 648:
A company runs its application on Oracle Database Enterprise Edition. The company needs to migrate the application and the database to AWS. The company can use the Bring Your Own License (BYOL) model while migrating to AWS. The application uses third-party database features that require privileged access. A solutions architect must design a solution for the database migration. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Migrate the database to Amazon RDS for Oracle by using native tools. Replace the third-party features with AWS Lambda.
B.Migrate the database to Amazon RDS Custom for Oracle by using native tools. Customize the new database settings to support the third-party features.
C.Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Customize the new database settings to support the third-party features.
D.Migrate the database to Amazon RDS for PostgreSQL by using AWS Database Migration Service (AWS DMS). Rewrite the application code to remove the dependency on third-party features.

Answer: B

Explanation:

- B is correct because RDS Custom for Oracle supports BYOL and privileged features.

- A is wrong because standard RDS for Oracle doesn't allow custom privileged features.

- C is wrong because DynamoDB is not a relational DB replacement here.

- D is wrong because rewriting to PostgreSQL adds major effort.

Question 649:

A large international university has deployed all of its compute services in the AWS Cloud. These services include Amazon EC2, Amazon RDS, and Amazon DynamoDB. The university currently relies on many custom scripts to back up its infrastructure. However, the university wants to centralize management and automate data backups as much as possible by using AWS native options. Which solution will meet these requirements?

Options:

A.Use third-party backup software with an AWS Storage Gateway tape gateway virtual tape library.

B.Use AWS Backup to configure and monitor all backups for the services in use.

C.Use AWS Config to set lifecycle management to take snapshots of all data sources on a schedule.

D.Use AWS Systems Manager State Manager to manage the configuration and monitoring of backup tasks.

Answer: B

Explanation:

- B is correct because AWS Backup centralizes and automates backups for EC2, RDS, DynamoDB.

- A is wrong because third-party solutions increase overhead.

- C is wrong because Config is for compliance monitoring, not backups.

- D is wrong because State Manager is for configuration management.

Question 650:

A company wants to build a map of its IT infrastructure to identify and enforce policies on resources that pose security risks. The company's security team must be able to query data in the IT infrastructure map and quickly identify security risks. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A.Use Amazon RDS to store the data. Use SQL to query the data to identify security risks.

B.Use Amazon Neptune to store the data. Use SPARQL to query the data to identify security risks.

C.Use Amazon Redshift to store the data. Use SQL to query the data to identify security risks.

D.Use Amazon DynamoDB to store the data. Use PartiQL to query the data to identify security risks.

Answer: B

Explanation:

- B is correct because Neptune supports graph databases, ideal for infrastructure mapping and relationship queries.

- A is wrong because RDS relational DBs are inefficient for graph relationships.

- C is wrong because Redshift is optimized for analytics, not graph traversal.

- D is wrong because DynamoDB is not efficient for complex relationship queries.

Question 651:

A large company wants to provide its globally located developers separate, limited size, managed PostgreSQL databases for development purposes. The databases will be low volume. The developers need the databases only when they are actively working. Question: 849 CertyIQ Question: 850 CertyIQ Question: 851 CertyIQ Which solution will meet these requirements MOST cost-effectively?

Options:

A.Give the developers the ability to launch separate Amazon Aurora instances. Set up a process to shut down Aurora instances at the end of the workday and to start Aurora instances at the beginning of the next workday.

B.Develop an AWS Service Catalog product that enforces size restrictions for launching Amazon Aurora instances. Give the developers access to launch the product when they need a development database.

C.Create an Amazon Aurora Serverless cluster. Develop an AWS Service Catalog product to launch databases in the cluster with the default capacity settings. Grant the developers access to the product.

D.Monitor AWS Trusted Advisor checks for idle Amazon RDS databases. Create a process to terminate identified idle RDS databases.

Answer: B

Explanation:

- B is correct because Service Catalog can enforce limits and give developers self-service access on-demand.

- A is wrong because shutting down and starting Aurora instances still incurs costs.

- C is wrong because Aurora Serverless default capacity may exceed cost needs and Service Catalog adds complexity.

- D is wrong because monitoring idle databases is reactive, not cost-effective upfront.

Question 652:

A company is building a web application that serves a content management system. The content management system runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across multiple Availability Zones. Users are constantly adding and updating files, blogs, and other website assets in the content management system. A solutions architect must implement a solution in which all the EC2 instances share up-to-date website content with the least possible lag time. Which solution meets these requirements?

Options:

A.Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently. Configure the ALB to make changes to the website assets only in the newest EC2 instance.

B.Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system. Configure each EC2 instance to mount the EFS file system locally. Configure the website hosting application to reference the website assets that are stored in the EFS file system.

C.Copy the website assets to an Amazon S3 bucket. Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume. Run the S3 sync command once each hour to keep files up to date.

D.Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets. Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched. Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume.

Answer: B

Explanation:

- B is correct because EFS provides a shared, consistent, low-latency file system across instances.

- A is wrong because syncing only from the newest instance is unreliable.

- C is wrong because hourly syncs cause lag and are not real-time.

- D is wrong because snapshots are static and do not update in real time.

Question 653:
A company's web application consists of multiple Amazon EC2 instances that run behind an Application Load Balancer in a VPC. An Amazon RDS for MySQL DB instance contains the data. The company needs the ability to automatically detect and respond to suspicious or unexpected behavior in its AWS environment. The company already has added AWS WAF to its architecture. What should a solutions architect do next to protect against threats?

Options:
A.Use Amazon GuardDuty to perform threat detection. Configure Amazon EventBridge to filter for GuardDuty findings and to invoke an AWS Lambda function to adjust the AWS WAF rules.
B.Use AWS Firewall Manager to perform threat detection. Configure Amazon EventBridge to filter for Firewall Manager findings and to invoke an AWS Lambda function to adjust the AWS WAF web ACL.
C.Use Amazon Inspector to perform threat detection and to update the AWS WAF rules. Create a VPC network ACL to limit access to the web application.
D.Use Amazon Macie to perform threat detection and to update the AWS WAF rules. Create a VPC network ACL to limit access to the web application.

Answer: A

Explanation:

- A is correct because GuardDuty provides continuous threat detection and integrates with EventBridge.

- B is wrong because Firewall Manager manages policies, not detection.

- C is wrong because Inspector checks vulnerabilities, not threats.

- D is wrong because Macie focuses on sensitive data, not threat detection.

Question 654:
A company is planning to run a group of Amazon EC2 instances that connect to an Amazon Aurora database. The company has built an AWS CloudFormation template to deploy the EC2 instances and the Aurora DB cluster. The company wants to allow the instances to authenticate to the database in a secure way. The company does not want to maintain static database credentials. Which solution meets these requirements with the LEAST operational effort?

Options:
A.Create a database user with a user name and password. Add parameters for the database user name and password to the CloudFormation template. Pass the parameters to the EC2 instances when the instances are launched.
B.Create a database user with a user name and password. Store the user name and password in AWS Systems Manager Parameter Store. Configure the EC2 instances to retrieve the database credentials from Parameter Store.
C.Configure the DB cluster to use IAM database authentication. Create a database user to use with IAM authentication. Associate a role with the EC2 instances to allow applications on the instances to access the database.
D.Configure the DB cluster to use IAM database authentication with an IAM user. Create a database user that has a name that matches the IAM user. Associate the IAM user with the EC2 instances to allow applications on the instances to access the database.

Answer: C

Explanation:

- C is correct because IAM database authentication avoids static credentials and integrates with EC2 roles.

- A is wrong because hardcoding credentials increases risk.

- B is wrong because Parameter Store still requires credential management.

- D is wrong because IAM users cannot be directly attached to EC2.

Question 655:
A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution. Which solution will deploy the certificate without incurring any additional costs?

Options:
A.Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
B.Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.
C.Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
D.Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.

Answer: C

Explanation:

- C is correct because CloudFront requires public certificates from ACM in us-east-1 at no cost.

- A is wrong because private certs in ACM are used for internal/private use only.

- B is wrong because region us-west-1 does not work for CloudFront.

- D is wrong for the same reason as B.

Question 656:
A company creates operations data and stores the data in an Amazon S3 bucket. For the company's annual audit, an external consultant needs to access an annual report that is stored in the S3 bucket. The external consultant needs to access the report for 7 days. The company must implement a solution to allow the external consultant access to only the report. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Create a new S3 bucket that is configured to host a public static website. Migrate the operations data to the new S3 bucket. Share the S3 website URL with the external consultant.
B.Enable public access to the S3 bucket for 7 days. Remove access to the S3 bucket when the external consultant completes the audit.
C.Create a new IAM user that has access to the report in the S3 bucket. Provide the access keys to the external consultant. Revoke the access keys after 7 days.
D.Generate a presigned URL that has the required access to the location of the report on the S3 bucket. Share the presigned URL with the external consultant.

Answer: D
Explanation:

- D is correct because presigned URLs provide time-limited, secure access without user creation.

- A is wrong because hosting public websites exposes all data.

- B is wrong because enabling public access violates security.

- C is wrong because IAM user creation adds overhead.

Question 657:
A company plans to run a high performance computing (HPC) workload on Amazon EC2 Instances. The workload requires low-latency network performance and high network throughput with tightly coupled node-to-node communication. Which solution will meet these requirements?

Options:
A.Configure the EC2 instances to be part of a cluster placement group.
B.Launch the EC2 instances with Dedicated Instance tenancy.
C.Launch the EC2 instances as Spot Instances.
D.Configure an On-Demand Capacity Reservation when the EC2 instances are launched.

Answer: A
Explanation:

- A is correct because cluster placement groups provide low-latency, high-bandwidth networking.

- B is wrong because Dedicated Instances are for isolation, not performance.

- C is wrong because Spot only impacts pricing, not network latency.

- D is wrong because capacity reservations don't guarantee low latency.

Question 658:
A company has primary and secondary data centers that are 500 miles (804.7 km) apart and interconnected with high-speed fiber-optic cable. The company needs a highly available and secure network connection between its data centers and a VPC on AWS for a mission-critical workload. A solutions architect must choose a connection solution that provides maximum resiliency. Which solution meets these requirements?

Options:
A.Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
B.A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
C.Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
D.A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Answer: C

Explanation:

- C is correct because multiple DX connections from both DCs into separate devices/locations provide max resiliency.

- A is wrong because it only uses primary DC.

- B is wrong because same device is single point of failure.

- D is wrong because fewer connections reduce resiliency.

Question 659:
A company runs several Amazon RDS for Oracle On-Demand DB instances that have high utilization. The RDS DB instances run in member accounts that are in an organization in AWS Organizations. The company's finance team has access to the organization's management account and member accounts. The finance team wants to find ways to optimize costs by using AWS Trusted Advisor. Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Use the Trusted Advisor recommendations in the management account.
B.Use the Trusted Advisor recommendations in the member accounts where the RDS DB instances are running.
C.Review the Trusted Advisor checks for Amazon RDS Reserved Instance Optimization.
D.Review the Trusted Advisor checks for Amazon RDS Idle DB Instances.
E.Review the Trusted Advisor checks for compute optimization. Crosscheck the results by using AWS Compute Optimizer.

Answer: AC

Explanation:

- A is correct because management account has org-level visibility.

- C is correct because RDS RI Optimization saves costs on high utilization.

- B is wrong because Trusted Advisor should be centralized.

- D is wrong because DBs are high utilization, not idle.

- E is wrong because compute optimization applies to EC2, not RDS.

Question 660:
A solutions architect is creating an application. The application will run on Amazon EC2 instances in private subnets across multiple Availability Zones in a VPC. The EC2 instances will frequently access large files that contain confidential information. These files are stored in Amazon S3 buckets for processing. The solutions architect must optimize the network architecture to minimize data transfer costs. What should the solutions architect do to meet these requirements?

Options:
A.Create a gateway endpoint for Amazon S3 in the VPC. In the route tables for the private subnets, add an entry for the gateway endpoint.
B.Create a single NAT gateway in a public subnet. In the route tables for the private subnets, add a default route that points to the NAT gateway.
C.Create an AWS PrivateLink interface endpoint for Amazon S3 in the VPIn the route tables for the private subnets, add an entry for the interface endpoint.
D.Create one NAT gateway for each Availability Zone in public subnets. In each of the route tables for the private subnets, add a default route that points to the NAT gateway in the same Availability Zone.

Answer: A

Explanation:

- A is correct because S3 gateway endpoint is free and minimizes transfer costs.

- B is wrong because NAT adds cost and uses internet.

- C is wrong because PrivateLink is unnecessary for S3.

- D is wrong because NAT per AZ adds more costs.

Question 661:
A company wants to relocate its on-premises MySQL database to AWS. The database accepts regular imports from a client-facing application, which causes a high volume of write operations. The company is concerned that the amount of traffic might be causing performance issues within the application. How should a solutions architect design the architecture on AWS?

Options:
A.Provision an Amazon RDS for MySQL DB instance with Provisioned IOPS SSD storage. Monitor write operation metrics by using Amazon CloudWatch. Adjust the provisioned IOPS if necessary.
B.Provision an Amazon RDS for MySQL DB instance with General Purpose SSD storage. Place an Amazon ElastiCache cluster in front of the DB instance. Configure the application to query ElastiCache instead.
C.Provision an Amazon DocumentDB (with MongoDB compatibility) instance with a memory optimized instance type. Monitor Amazon CloudWatch for performance-related issues. Change the instance class if necessary.
D.Provision an Amazon Elastic File System (Amazon EFS) file system in General Purpose performance mode. Monitor Amazon CloudWatch for IOPS bottlenecks. Change to Provisioned Throughput performance mode if necessary.

Answer: A

Explanation:

- A is correct because RDS with Provisioned IOPS ensures high write throughput.

- B is wrong because ElastiCache is for reads, not writes.

- C is wrong because DocumentDB is not MySQL compatible.

- D is wrong because EFS is unrelated to DB workloads.

Question 662:
A company runs an application in the AWS Cloud that generates sensitive archival data files. The company wants to rearchitect the application's data storage. The company wants to encrypt the data files and to ensure that third parties do not have access to the data before the data is encrypted and sent to AWS. The company has already created an Amazon S3 bucket. Which solution will meet these requirements?

Options:
A.Configure the S3 bucket to use client-side encryption with an Amazon S3 managed encryption key. Configure the application to use the S3 bucket to store the archival files.
B.Configure the S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Configure the application to use the S3 bucket to store the archival files.
C.Configure the S3 bucket to use dual-layer server-side encryption with AWS KMS keys (SSE-KMS). Configure the application to use the S3 bucket to store the archival files.
D.Configure the application to use client-side encryption with a key stored in AWS Key Management Service (AWS KMS). Configure the application to store the archival files in the S3 bucket.

Answer: D
Explanation:

- D is correct because client-side encryption ensures data is encrypted before AWS receives it.

- A is wrong because S3 managed keys are server-side, not client-side.

- B is wrong because SSE-KMS encrypts only after AWS receives the data.

- C is wrong because dual-layer SSE still means encryption occurs server-side.

Question 663:
A company uses Amazon RDS with default backup settings for its database tier. The company needs to make a daily backup of the database to meet regulatory requirements. The company must retain the backups for 30 days. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Write an AWS Lambda function to create an RDS snapshot every day.
B.Modify the RDS database to have a retention period of 30 days for automated backups.
C.Use AWS Systems Manager Maintenance Windows to modify the RDS backup retention period.
D.Create a manual snapshot every day by using the AWS CLI. Modify the RDS backup retention period.

Answer: B
Explanation:

- B is correct because RDS automated backups can be configured with a retention period up to 35 days.

- A is wrong because Lambda adds unnecessary automation complexity.

- C is wrong because Maintenance Windows is not used for DB backup retention.

- D is wrong because manual snapshots require daily manual or scripted effort.

Question 664:
A company that runs its application on AWS uses an Amazon Aurora DB cluster as its database. During peak usage hours when multiple users access and read the data, the monitoring system shows degradation of database performance for the write queries. The company wants to increase the scalability of the application to meet peak usage demands. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create a second Aurora DB cluster. Configure a copy job to replicate the users' data to the new database. Update the application to use the second database to read the data.
B.Create an Amazon DynamoDB Accelerator (DAX) cluster in front of the existing Aurora DB cluster. Update the application to use the DAX cluster for read-only queries. Write data directly to the Aurora DB cluster.
C.Create an Aurora read replica in the existing Aurora DB cluster. Update the application to use the replica endpoint for read-only queries and to use the cluster endpoint for write queries.
D.Create an Amazon Redshift cluster. Copy the users' data to the Redshift cluster. Update the application to connect to the Redshift cluster and to perform read-only queries on the Redshift cluster.

Answer: C
Explanation:

- C is correct because Aurora replicas handle read queries, offloading load from the writer.

- A is wrong because maintaining a second cluster doubles costs.

- B is wrong because DAX is for DynamoDB, not Aurora.

- D is wrong because Redshift is for analytics, not OLTP workloads.

Question 665:
A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance. Which combination of steps should the solutions architect take? (Choose two.)

Options:
A.Use Amazon Kinesis Data Firehose to ingest the data.
B.Use AWS Lambda with AWS Step Functions to process the data.
C.Use AWS Database Migration Service (AWS DMS) to ingest the data.
D.Use Amazon EC2 instances in an Auto Scaling group to process the data.
E.Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Answer: AE
Explanation:

- A is correct because Kinesis Data Firehose scales ingestion automatically.

- E is correct because Fargate provides scalable containerized processing.

- B is wrong because Step Functions + Lambda is not efficient for long-running jobs.

- C is wrong because DMS is for DB migration, not streaming ingestion.

- D is wrong because EC2 Auto Scaling requires more management overhead.

Question 666:

A company runs a web application on multiple Amazon EC2 instances in a VPC. The application needs to write sensitive data to an Amazon S3 bucket. The data cannot be sent over the public internet. Which solution will meet these requirements?

Options:

A.Create a gateway VPC endpoint for Amazon S3. Create a route in the VPC route table to the endpoint.

B.Create an internal Network Load Balancer that has the S3 bucket as the target.

C.Deploy the S3 bucket inside the VPCreate a route in the VPC route table to the bucket.

D.Create an AWS Direct Connect connection between the VPC and an S3 regional endpoint.

Answer: A

Explanation:

- A is correct because an S3 gateway endpoint enables private connectivity to S3 without internet.

- B is wrong because S3 is not a load balancer target.

- C is wrong because S3 cannot be deployed inside a VPC.

- D is wrong because Direct Connect is costly for this case.

Question 667:

A company runs its production workload on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) volumes. A solutions architect needs to analyze the current EBS volume cost and to recommend optimizations. The recommendations need to include estimated monthly saving opportunities. Which solution will meet these requirements?

Options:

A.Use Amazon Inspector reporting to generate EBS volume recommendations for optimization.

B.Use AWS Systems Manager reporting to determine EBS volume recommendations for optimization.

C.Use Amazon CloudWatch metrics reporting to determine EBS volume recommendations for optimization.

D.Use AWS Compute Optimizer to generate EBS volume recommendations for optimization.

Answer: D

Explanation:

- D is correct because Compute Optimizer provides EBS optimization recommendations with savings.

- A is wrong because Inspector focuses on vulnerabilities, not cost.

- B is wrong because Systems Manager is not for cost analysis.

- C is wrong because CloudWatch provides metrics but no optimization guidance.

Question 668:

A global company runs its workloads on AWS. The company's application uses Amazon S3 buckets across AWS Regions for sensitive data storage and analysis. The company stores millions of objects in multiple S3 buckets daily. The company wants to identify all S3 buckets that are not versioning-enabled. Which solution will meet these requirements?

Options:

B.Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions.

C.Enable IAM Access Analyzer for S3 to identify all S3 buckets that are not versioning-enabled across Regions.

D.Create an S3 Multi-Region Access Point to identify all S3 buckets that are not versioning-enabled across Regions.

Answer: B

Explanation:

- B is correct because S3 Storage Lens provides bucket-level insights including versioning status.

- C is wrong because Access Analyzer is for access policies, not versioning.

- D is wrong because Multi-Region Access Point manages access, not versioning status.

- A is missing from options, but Storage Lens is the best fit.

Question 669:

A company wants to enhance its ecommerce order-processing application that is deployed on AWS. The application must process each order exactly once without affecting the customer experience during unpredictable traffic surges. Which solution will meet these requirements?

Options:

A.Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Put all the orders in the SQS queue. Configure an AWS Lambda function as the target to process the orders.

B.Create an Amazon Simple Notification Service (Amazon SNS) standard topic. Publish all the orders to the SNS standard topic. Configure the application as a notification target.

C.Create a flow by using Amazon AppFlow. Send the orders to the flow. Configure an AWS Lambda function as the target to process the orders.

D.Configure AWS X-Ray in the application to track the order requests. Configure the application to process the orders by pulling the orders from Amazon CloudWatch.

Answer: A

Explanation:

- A is correct because SQS FIFO ensures exactly-once processing with Lambda scaling.

- B is wrong because SNS standard does not guarantee exactly-once delivery.

- C is wrong because AppFlow is for SaaS data integration, not order queueing.

- D is wrong because X-Ray is for tracing, not processing.

Question 670:
A company has two AWS accounts: Production and Development. The company needs to push code changes in the Development account to the Production account. In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers will need access to perform testing. Which solution will meet these requirements?

Options:
A.Create two policy documents by using the AWS Management Console in each account. Assign the policy to developers who need access.
B.Create an IAM role in the Development account. Grant the IAM role access to the Production account. Allow developers to assume the role.
C.Create an IAM role in the Production account. Define a trust policy that specifies the Development account. Allow developers to assume the role.
D.Create an IAM group in the Production account. Add the group as a principal in a trust policy that specifies the Production account. Add developers to the group.

Answer: C

Explanation:

- C is correct because cross-account IAM roles with trust policies are the proper solution.

- A is wrong because policies in each account don't provide cross-account access.

- B is wrong because roles granting access must exist in Production, not Development.

- D is wrong because IAM groups cannot be used as principals for cross-account trust.

Question 671:
A company wants to restrict access to the content of its web application. The company needs to protect the content by using authorization techniques that are available on AWS. The company also wants to implement a serverless architecture for authorization and authentication that has low login latency. The solution must integrate with the web application and serve web content globally. The application currently has a small user base, but the company expects the application's user base to increase. Which solution will meet these requirements?

Options:
A.Configure Amazon Cognito for authentication. Implement Lambda@Edge for authorization. Configure Amazon CloudFront to serve the web application globally.
B.Configure AWS Directory Service for Microsoft Active Directory for authentication. Implement AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
C.Configure Amazon Cognito for authentication. Implement AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
D.Configure AWS Directory Service for Microsoft Active Directory for authentication. Implement Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Answer: A

Explanation:

- A is correct because Cognito handles auth, Lambda@Edge enforces authorization, CloudFront distributes globally.

- B is wrong because AD + ALB is not serverless and adds overhead.

- C is wrong because Transfer Acceleration is for file uploads, not serving web apps.

- D is wrong because AD + Beanstalk is not scalable serverless auth.

Question 672:
A development team uses multiple AWS accounts for its development, staging, and production environments. Team members have been launching large Amazon EC2 instances that are underutilized. A solutions architect must prevent large instances from being launched in all accounts. How can the solutions architect meet this requirement with the LEAST operational overhead?

Options:
A.Update the IAM policies to deny the launch of large EC2 instances. Apply the policies to all users.
B.Define a resource in AWS Resource Access Manager that prevents the launch of large EC2 instances.
C.Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role.
D.Create an organization in AWS Organizations in the management account with the default policy. Create a service control policy (SCP) that denies the launch of large EC2 instances, and apply it to the AWS accounts.

Answer: D
Explanation:

- D is correct because SCPs in AWS Organizations centrally prevent actions across all accounts.

- A is wrong because updating IAM policies per user is manual and error-prone.

- B is wrong because Resource Access Manager doesn't block instance launches.

- C is wrong because managing per-account roles adds overhead.

Question 673:
A company has migrated a fleet of hundreds of on-premises virtual machines (VMs) to Amazon EC2 instances. The instances run a diverse fleet of Windows Server versions along with several Linux distributions. The company wants a solution that will automate inventory and updates of the operating systems. The company also needs a summary of common vulnerabilities of each instance for regular monthly reviews. What should a solutions architect recommend to meet these requirements?

Options:
A.Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Configure AWS Security Hub to produce monthly reports.
B.Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Deploy Amazon Inspector, and configure monthly reports.
C.Set up AWS Shield Advanced, and configure monthly reports. Deploy AWS Config to automate patch installations on the EC2 instances.
D.Set up Amazon GuardDuty in the account to monitor all EC2 instances. Deploy AWS Config to automate patch installations on the EC2 instances.

Answer: B
Explanation:

- B is correct because Patch Manager handles patching, Inspector provides vulnerability assessments.

- A is wrong because Security Hub aggregates findings, but Inspector is required for vulnerabilities.

- C is wrong because Shield Advanced is for DDoS protection.

- D is wrong because GuardDuty is for threat detection, not vulnerability scans.

Question 674:
A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer. The application connects to an Amazon DynamoDB table. For disaster recovery (DR) purposes, the company wants to ensure that the application is available from another AWS Region with minimal downtime. Which solution will meet these requirements with the LEAST downtime?
Options:
A.Create an Auto Scaling group and an ELB in the DR Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new DR Region's ELB.
B.Create an AWS CloudFormation template to create EC2 instances, ELBs, and DynamoDB tables to be launched when necessary. Configure DNS failover to point to the new DR Region's ELB.
C.Create an AWS CloudFormation template to create EC2 instances and an ELB to be launched when necessary. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new DR Region's ELB.
D.Create an Auto Scaling group and an ELB in the DR Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm with an evaluation period of 10 minutes to invoke an AWS Lambda function that updates Amazon Route 53 to point to the DR Region's ELB.
Answer: C
Explanation:

- C is correct because CloudFormation + DynamoDB global tables minimize downtime and automate setup.

- A is wrong because always-running DR infra adds cost.

- B is wrong because DynamoDB data must be replicated proactively.

- D is wrong because waiting for alarms adds more downtime.

Question 675:
A company runs an application on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3 buckets. According to regulatory requirements, the data must not travel across the public internet. What should a solutions architect do to meet these requirements MOST cost-effectively?
Options:
A.Deploy a NAT gateway to access the S3 buckets.
B.Deploy AWS Storage Gateway to access the S3 buckets.
C.Deploy an S3 interface endpoint to access the S3 buckets.
D.Deploy an S3 gateway endpoint to access the S3 buckets.
Answer: D
Explanation:

- D is correct because S3 gateway endpoints provide private connectivity to S3 at no cost.

- A is wrong because NAT gateways incur costs and use internet.

- B is wrong because Storage Gateway is for hybrid storage, not VPC S3 access.

- C is wrong because interface endpoints for S3 cost money; gateway endpoint is cheaper.

Question 676:
A company hosts an application on Amazon EC2 instances that run in a single Availability Zone. The application is accessible by using the transport layer of the Open Systems Interconnection (OSI) model. The company needs the application architecture to have high availability. Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)
Options:
A.Configure new EC2 instances in a different Availability Zone. Use Amazon Route 53 to route traffic to all instances.
B.Configure a Network Load Balancer in front of the EC2 instances.
C.Configure a Network Load Balancer for TCP traffic to the instances. Configure an Application Load Balancer for HTTP and HTTPS traffic to the instances.
D.Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group to use multiple Availability Zones. Configure the Auto Scaling group to run application health checks on the instances.
E.Create an Amazon CloudWatch alarm. Configure the alarm to restart EC2 instances that transition to a stopped state.
Answer: BD
Explanation:

- B is correct because a Network Load Balancer operates at the transport layer (OSI Layer 4).

- D is correct because Auto Scaling across multiple AZs ensures high availability.

- A is wrong because Route 53 alone does not provide health-based load balancing.

- C is wrong because using both NLB and ALB adds unnecessary cost/complexity.

Question 677:
A company uses Amazon S3 to host its static website. The company wants to add a contact form to the webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company expects fewer than 100 site visits each month. The contact form must notify the company by email when a customer fills out the form. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Host the dynamic contact form in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to a third-party email provider.
B.Create an Amazon API Gateway endpoint that returns the contact form from an AWS Lambda function. Configure another Lambda function on the API Gateway to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
C.Host the website by using AWS Amplify Hosting for static content and dynamic content. Use server-side scripting to build the contact form. Configure Amazon Simple Queue Service (Amazon SQS) to deliver the message to the company.
D.Migrate the website from Amazon S3 to Amazon EC2 instances that run Windows Server. Use Internet Information Services (IIS) for Windows Server to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
Answer: B
Explanation:

- B is correct because API Gateway + Lambda + SNS is serverless and cheap for low traffic.

- A is wrong because ECS adds unnecessary cost and complexity.

- C is wrong because Amplify is more expensive for such low usage.

- D is wrong because EC2 and IIS introduce high cost and overhead.

Question 678:
A company creates dedicated AWS accounts in AWS Organizations for its business units. Recently, an important notification was sent to the root user email address of a business unit account instead of the assigned account owner. The company wants to ensure that all future notifications can be sent to different employees based on the notification categories of billing, operations, or security. Which solution will meet these requirements MOST securely?

Options:
A.Configure each AWS account to use a single email address that the company manages. Ensure that all account owners can access the email account to receive notifications. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
B.Configure each AWS account to use a different email distribution list for each business unit that the company manages. Configure each distribution list with administrator email addresses that can respond to alerts. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
C.Configure each AWS account root user email address to be the individual company managed email address of one person from each business unit. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
D.Configure each AWS account root user to use email aliases that go to a centralized mailbox. Configure alternate contacts for each account by using a single business managed email distribution list each for the billing team, the security team, and the operations team.

Answer: A

Explanation:

- A is correct because alternate contacts separate billing, operations, and security properly.

- B is wrong because using multiple root email accounts creates confusion.

- C is wrong because root user emails should not be tied to individuals.

- D is wrong because centralized aliases defeat separation of duties.

Question 679:
A company runs an ecommerce application on AWS. Amazon EC2 instances process purchases and store the purchase details in an Amazon Aurora PostgreSQL DB cluster. Customers are experiencing application timeouts during times of peak usage. A solutions architect needs to rearchitect the application so that the application can scale to meet peak usage demands. Which combination of actions will meet these requirements MOST cost-effectively? (Choose two.)

Options:
A.Configure an Auto Scaling group of new EC2 instances to retry the purchases until the processing is complete. Update the applications to connect to the DB cluster by using Amazon RDS Proxy.
B.Configure the application to use an Amazon ElastiCache cluster in front of the Aurora PostgreSQL DB cluster.

C.Update the application to send the purchase requests to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an Auto Scaling group of new EC2 instances that read from the SQS queue.

D.Configure an AWS Lambda function to retry the ticket purchases until the processing is complete.

E.Configure an Amazon API Gateway REST API with a usage plan.

Answer: BC

Explanation:

- B is correct because ElastiCache reduces read load on Aurora.

- C is correct because SQS decouples processing from spikes in demand.

- A is wrong because retries do not solve scaling under heavy writes.

- D is wrong because Lambda is not suitable for long-running transactions.

Question 680:
A company that uses AWS Organizations runs 150 applications across 30 different AWS accounts. The company used AWS Cost and Usage Report to create a new report in the management account. The report is delivered to an Amazon S3 bucket that is replicated to a bucket in the data collection account. The company's senior leadership wants to view a custom dashboard that provides NAT gateway costs each day starting at the beginning of the current month. Which solution will meet these requirements?

Options:
A.Share an Amazon QuickSight dashboard that includes the requested table visual. Configure QuickSight to use AWS DataSync to query the new report.

B.Share an Amazon QuickSight dashboard that includes the requested table visual. Configure QuickSight to use Amazon Athena to query the new report.

C.Share an Amazon CloudWatch dashboard that includes the requested table visual. Configure CloudWatch to use AWS DataSync to query the new report.

D.Share an Amazon CloudWatch dashboard that includes the requested table visual. Configure CloudWatch to use Amazon Athena to query the new report.

Answer: B

Explanation:

- B is correct because QuickSight + Athena is the right way to visualize CUR data.

- A is wrong because DataSync is for file transfers, not querying.

- C is wrong because CloudWatch cannot directly query CUR.

- D is wrong because CloudWatch does not integrate with Athena.

Question 681:
A company is hosting a high-traffic static website on Amazon S3 with an Amazon CloudFront distribution that has a default TTL of 0 seconds. The company wants to implement caching to improve performance for the website. However, the company also wants to ensure that stale content is not served for more than a few minutes after a deployment. Which combination of caching methods should a solutions architect implement to meet these requirements? (Choose two.)

Options:
A.Set the CloudFront default TTL to 2 minutes.
B.Set a default TTL of 2 minutes on the S3 bucket.
C.Add a Cache-Control private directive to the objects in Amazon S3.
D.Create an AWS Lambda@Edge function to add an Expires header to HTTP responses.
Configure the function to run on viewer response.
E.Add a Cache-Control max-age directive of 24 hours to the objects in Amazon S3. On
deployment, create a CloudFront invalidation to clear any changed files from edge caches.
Answer: AC
Explanation:

- A is correct because a short CloudFront TTL ensures fresh updates.

- C is correct because Cache-Control directives control caching behavior.

- B is wrong because S3 does not set cache TTLs for CloudFront.

- D is wrong because Lambda@Edge is unnecessary here.

Question 682:
A company runs its application by using Amazon EC2 instances and AWS Lambda functions.
The EC2 instances run in private subnets of a VPC. The Lambda functions need direct network
access to the EC2 instances for the application to work. The application will run for 1 year. The
number of Lambda functions that the application uses will increase during the 1-year period.
The company must minimize costs on all application resources. Which solution will meet these
requirements?
Options:
A.Purchase an EC2 Instance Savings Plan. Connect the Lambda functions to the private
subnets that contain the EC2 instances.
B.Purchase an EC2 Instance Savings Plan. Connect the Lambda functions to new public
subnets in the same VPC where the EC2 instances run.
C.Purchase a Compute Savings Plan. Connect the Lambda functions to the private subnets
that contain the EC2 instances.
D.Purchase a Compute Savings Plan. Keep the Lambda functions in the Lambda service VPC.
Answer: C
Explanation:

- C is correct because Compute Savings Plans apply to both EC2 and Lambda.

- A is wrong because EC2 Instance Plans only apply to EC2, not Lambda.

- B is wrong because Lambda in public subnets is not correct.

- D is wrong because Lambda must connect privately to EC2.

Question 683:
A company has deployed a multi-account strategy on AWS by using AWS Control Tower. The company has provided individual AWS accounts to each of its developers. The company wants to implement controls to limit AWS resource costs that the developers incur. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Instruct each developer to tag all their resources with a tag that has a key of CostCenter and a value of the developer's name. Use the required-tags AWS Config managed rule to check for the tag. Create an AWS Lambda function to terminate resources that do not have the tag. Configure AWS Cost Explorer to send a daily report to each developer to monitor their spending.
B.Use AWS Budgets to establish budgets for each developer account. Set up budget alerts for actual and forecast values to notify developers when they exceed or expect to exceed their assigned budget. Use AWS Budgets actions to apply a DenyAll policy to the developer's IAM role to prevent additional resources from being launched when the assigned budget is reached.
C.Use AWS Cost Explorer to monitor and report on costs for each developer account. Configure Cost Explorer to send a daily report to each developer to monitor their spending. Use AWS Cost Anomaly Detection to detect anomalous spending and provide alerts.
D.Use AWS Service Catalog to allow developers to launch resources within a limited cost range. Create AWS Lambda functions in each AWS account to stop running resources at the end of each work day. Configure the Lambda functions to resume the resources at the start of each work day.
Answer: B
Explanation:

- B is correct because AWS Budgets with actions automates enforcement.

- A is wrong because tagging + Lambda termination adds too much overhead.

- C is wrong because reporting only alerts, does not enforce limits.

- D is wrong because Service Catalog + Lambda requires per-account setup.

Question 684:
A solutions architect is designing a three-tier web application. The architecture consists of an internet-facing Application Load Balancer (ALB) and a web tier that is hosted on Amazon EC2 instances in private subnets. The application tier with the business logic runs on EC2 instances in private subnets. The database tier consists of Microsoft SQL Server that runs on EC2 instances in private subnets. Security is a high priority for the company. Which combination of security group configurations should the solutions architect use? (Choose three.)
Options:
A.Configure the security group for the web tier to allow inbound HTTPS traffic from the security group for the ALB.
B.Configure the security group for the web tier to allow outbound HTTPS traffic to 0.0.0.0/0.
C.Configure the security group for the database tier to allow inbound Microsoft SQL Server traffic from the security group for the application tier.
D.Configure the security group for the database tier to allow outbound HTTPS traffic and Microsoft SQL Server traffic to the security group for the web tier.
E.Configure the security group for the application tier to allow inbound HTTPS traffic from the security group for the web tier.
F.Configure the security group for the application tier to allow outbound HTTPS traffic and Microsoft SQL Server traffic to the security group for the web tier.

Answer: ACE

Explanation:

- A is correct because ALB → web tier must be allowed.

- C is correct because app tier → DB tier must be allowed for SQL Server.

- E is correct because web tier → app tier must be allowed.

- B is wrong because web tier outbound 0.0.0.0/0 is too open.

Question 685:

A company has released a new version of its production application. The company's workload uses Amazon EC2, AWS Lambda, AWS Fargate, and Amazon SageMaker. The company wants to cost optimize the workload now that usage is at a steady state. The company wants to cover the most services with the fewest savings plans. Which combination of savings plans will meet these requirements? (Choose two.)

Options:

A.Purchase an EC2 Instance Savings Plan for Amazon EC2 and SageMaker.
B.Purchase a Compute Savings Plan for Amazon EC2, Lambda, and SageMaker.
C.Purchase a SageMaker Savings Plan.
D.Purchase a Compute Savings Plan for Lambda, Fargate, and Amazon EC2.
E.Purchase an EC2 Instance Savings Plan for Amazon EC2 and Fargate.

Answer: CD

Explanation:

- C is correct because SageMaker requires its own savings plan.

- D is correct because Compute Savings Plan covers EC2, Lambda, and Fargate.

- A is wrong because EC2 Instance Plan does not apply to SageMaker.

- B is wrong because SageMaker is excluded from Compute Plan.

Question 686:

A company uses a Microsoft SQL Server database. The company's applications are connected to the database. The company wants to migrate to an Amazon Aurora PostgreSQL database with minimal changes to the application code. Which combination of steps will meet these requirements? (Choose two.)

Options:

A.Use the AWS Schema Conversion Tool (AWS SCT) to rewrite the SQL queries in the applications.
B.Enable Babelfish on Aurora PostgreSQL to run the SQL queries from the applications.
C.Migrate the database schema and data by using the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS).
D.Use Amazon RDS Proxy to connect the applications to Aurora PostgreSQL.
E.Use AWS Database Migration Service (AWS DMS) to rewrite the SQL queries in the applications.

Answer: BC

Explanation:

- B is correct because Babelfish allows SQL Server queries on Aurora PostgreSQL.

- C is correct because SCT + DMS migrate schema and data.

- A is wrong because SCT does not rewrite application SQL queries directly.

- D is wrong because RDS Proxy helps with pooling, not migration.

Question 687:

A company plans to rehost an application to Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) as the attached storage. A solutions architect must design a solution to ensure that all newly created Amazon EBS volumes are encrypted by default. The solution must also prevent the creation of unencrypted EBS volumes. Which solution will meet these requirements?

Options:

A.Configure the EC2 account attributes to always encrypt new EBS volumes.

B.Use AWS Config. Configure the encrypted-volumes identifier. Apply the default AWS Key Management Service (AWS KMS) key.

C.Configure AWS Systems Manager to create encrypted copies of the EBS volumes. Reconfigure the EC2 instances to use the encrypted volumes.

D.Create a customer managed key in AWS Key Management Service (AWS KMS). Configure AWS Migration Hub to use the key when the company migrates workloads.

Answer: B

Explanation:

- B is correct because AWS Config can enforce compliance with encryption requirement.

- A is wrong because account attributes alone don't prevent unencrypted volumes.

- C is wrong because Systems Manager copies volumes after creation.

- D is wrong because Migration Hub is for tracking, not enforcing encryption.

Question 688:

An ecommerce company wants to collect user clickstream data from the company's website for real-time analysis. The website experiences fluctuating traffic patterns throughout the day. The company needs a scalable solution that can adapt to varying levels of traffic. Which solution will meet these requirements?

Options:

A.Use a data stream in Amazon Kinesis Data Streams in on-demand mode to capture the clickstream data. Use AWS Lambda to process the data in real time.

B.Use Amazon Kinesis Data Firehose to capture the clickstream data. Use AWS Glue to process the data in real time.

C.Use Amazon Kinesis Video Streams to capture the clickstream data. Use AWS Glue to process the data in real time.

D.Use Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) to capture the clickstream data. Use AWS Lambda to process the data in real time.

Answer: A

Explanation:

- A is correct because Kinesis Data Streams on-demand mode scales automatically.

- B is wrong because Firehose is for delivery, not real-time processing.

- C is wrong because Video Streams is for video, not click data.

- D is wrong because Flink consumes data, not captures.

Question 689:
A global company runs its workloads on AWS. The company's application uses Amazon S3 buckets across AWS Regions for sensitive data storage and analysis. The company stores millions of objects in multiple S3 buckets daily. The company wants to identify all S3 buckets that are not versioning-enabled. Which solution will meet these requirements?
Options:
A.Set up an AWS CloudTrail event that has a rule to identify all S3 buckets that are not versioning-enabled across Regions.
B.Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions.
C.Enable IAM Access Analyzer for S3 to identify all S3 buckets that are not versioning-enabled across Regions.
D.Create an S3 Multi-Region Access Point to identify all S3 buckets that are not versioning-enabled across Regions.
Answer: B
Explanation:

- B is correct because S3 Storage Lens provides insights on bucket configurations including versioning.

- A is wrong because CloudTrail tracks events, not versioning status.

- C is wrong because Access Analyzer is for access permissions.

- D is wrong because MRAP is for access, not versioning insights.

Question 690:
A company needs to optimize its Amazon S3 storage costs for an application that generates many files that cannot be recreated. Each file is approximately 5 MB and is stored in Amazon S3 Standard storage. The company must store the files for 4 years before the files can be deleted. The files must be immediately accessible. The files are frequently accessed in the first 30 days of object creation, but they are rarely accessed after the first 30 days. Which solution will meet these requirements MOST cost-effectively?
Options:
A.Create an S3 Lifecycle policy to move the files to S3 Glacier Instant Retrieval 30 days after object creation. Delete the files 4 years after object creation.
B.Create an S3 Lifecycle policy to move the files to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days after object creation. Delete the files 4 years after object creation.
C.Create an S3 Lifecycle policy to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days after object creation. Delete the files 4 years after object creation.
D.Create an S3 Lifecycle policy to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days after object creation. Move the files to S3 Glacier Flexible Retrieval 4 years after object creation.
Answer: A
Explanation:

- A is correct because Glacier Instant Retrieval provides immediate access with lower cost.

- B is wrong because One Zone-IA has durability risks.

- C is wrong because Standard-IA is more expensive than Glacier IR for long term.

- D is wrong because Glacier Flexible Retrieval adds retrieval delays.

Question 691:
A company runs its critical storage application in the AWS Cloud. The application uses Amazon S3 in two AWS Regions. The company wants the application to send remote user data to the nearest S3 bucket with no public network congestion. The company also wants the application to fail over with the least amount of management of Amazon S3. Which solution will meet these requirements?

Options:
A.Implement an active-active design between the two Regions. Configure the application to use the regional S3 endpoints closest to the user.
B.Use an active-passive configuration with S3 Multi-Region Access Points. Create a global endpoint for each of the Regions.
C.Send user data to the regional S3 endpoints closest to the user. Configure an S3 cross-account replication rule to keep the S3 buckets synchronized.
D.Set up Amazon S3 to use Multi-Region Access Points in an active-active configuration with a single global endpoint. Configure S3 Cross-Region Replication.

Answer: D
Explanation:

- D is correct because MRAP provides global endpoint + failover management.

- A is wrong because app changes are required.

- B is wrong because active-passive introduces failover complexity.

- C is wrong because replication doesn't handle user routing.

Question 692:
A company is migrating a data center from its on-premises location to AWS. The company has several legacy applications that are hosted on individual virtual servers. Changes to the application designs cannot be made. Each individual virtual server currently runs as its own EC2 instance. A solutions architect needs to ensure that the applications are reliable and fault tolerant after migration to AWS. The applications will run on Amazon EC2 instances. Which solution will meet these requirements?

Options:
A.Create an Auto Scaling group that has a minimum of one and a maximum of one. Create an Amazon Machine Image (AMI) of each application instance. Use the AMI to create EC2 instances in the Auto Scaling group. Configure an Application Load Balancer in front of the Auto Scaling group.
B.Use AWS Backup to create an hourly backup of the EC2 instance that hosts each application. Store the backup in Amazon S3 in a separate Availability Zone. Configure a disaster recovery process to restore the EC2 instance for each application from its most recent backup.
C.Create an Amazon Machine Image (AMI) of each application instance. Launch two new EC2 instances from the AMI. Place each EC2 instance in a separate Availability Zone. Configure a Network Load Balancer that has the EC2 instances as targets.
D.Use AWS Migration Hub Refactor Spaces to migrate each application off the EC2 instance. Break down functionality from each application into individual components. Host each application on Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type.

Answer: C
Explanation:

- C is correct because running 2 instances across AZs with NLB ensures HA and fault tolerance.

- A is wrong because ASG min=1 max=1 provides no redundancy.

- B is wrong because restores introduce downtime.

- D is wrong because refactoring is not allowed.

Question 693:
A company wants to isolate its workloads by creating an AWS account for each workload. The company needs a solution that centrally manages networking components for the workloads. The solution also must create accounts with automatic security controls (guardrails). Which solution will meet these requirements with the LEAST operational overhead?
Options:
A.Use AWS Control Tower to deploy accounts. Create a networking account that has a VPC with private subnets and public subnets. Use AWS Resource Access Manager (AWS RAM) to share the subnets with the workload accounts.
B.Use AWS Organizations to deploy accounts. Create a networking account that has a VPC with private subnets and public subnets. Use AWS Resource Access Manager (AWS RAM) to share the subnets with the workload accounts.
C.Use AWS Control Tower to deploy accounts. Deploy a VPC in each workload account. Configure each VPC to route through an inspection VPC by using a transit gateway attachment.
D.Use AWS Organizations to deploy accounts. Deploy a VPC in each workload account. Configure each VPC to route through an inspection VPC by using a transit gateway attachment.
Answer: A
Explanation:

- A is correct because Control Tower provides account provisioning + guardrails with RAM for networking.

- B is wrong because Organizations alone lacks guardrails.

- C is wrong because deploying VPCs in every account increases overhead.

- D is wrong because Organizations does not enforce guardrails.

Question 694:
A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing. The company wants to minimize the website hosting costs. Which solution will meet these requirements?
Options:
A.Move the website to an Amazon S3 bucket. Configure an Amazon CloudFront distribution for the S3 bucket.
B.Move the website to an Amazon S3 bucket. Configure an Amazon ElastiCache cluster for the S3 bucket.
C.Move the website to AWS Amplify. Configure an ALB to resolve to the Amplify website.
D.Move the website to AWS Amplify. Configure EC2 instances to cache the website.
Answer: A

Explanation:

- A is correct because S3 + CloudFront is cheapest and scales well for static sites.

- B is wrong because ElastiCache is not used with S3.

- C is wrong because Amplify is more expensive for static hosting.

- D is wrong because EC2 caching adds cost.

Question 695:
A company is implementing a shared storage solution for a media application that the company hosts on AWS. The company needs the ability to use SMB clients to access stored data. Which solution will meet these requirements with the LEAST administrative overhead?
Options:
A.Create an AWS Storage Gateway Volume Gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
B.Create an AWS Storage Gateway Tape Gateway. Configure tapes to use Amazon S3. Connect the application server to the Tape Gateway.
C.Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
D.Create an Amazon FSx for Windows File Server file system. Connect the application server to the file system.
Answer: D
Explanation:

- D is correct because FSx for Windows is fully managed SMB storage.

- A is wrong because Volume Gateway is for block storage.

- B is wrong because Tape Gateway is for backups.

- C is wrong because managing EC2 adds overhead.

Question 696:
A company is designing its production application's disaster recovery (DR) strategy. The application is backed by a MySQL database on an Amazon Aurora cluster in the us-east-1 Region. The company has chosen the us-west-1 Region as its DR Region. The company's target recovery point objective (RPO) is 5 minutes and the target recovery time objective (RTO) is 20 minutes. The company wants to minimize configuration changes. Which solution will meet these requirements with the MOST operational efficiency?
Options:
A.Create an Aurora read replica in us-west-1 similar in size to the production application's Aurora MySQL cluster writer instance.
B.Convert the Aurora cluster to an Aurora global database. Configure managed failover.
C.Create a new Aurora cluster in us-west-1 that has Cross-Region Replication.
D.Create a new Aurora cluster in us-west-1. Use AWS Database Migration Service (AWS DMS) to sync both clusters.
Answer: B
Explanation:

- B is correct because Aurora Global DB offers <1 minute RPO and quick failover.

- A is wrong because cross-Region read replicas have longer replication lag.

- C is wrong because CRR is manual setup.

- D is wrong because DMS adds overhead.

Question 697:
A company runs a critical data analysis job each week before the first day of the work week. The job requires at least 1 hour to complete the analysis. The job is stateful and cannot tolerate interruptions. The company needs a solution to run the job on AWS. Which solution will meet these requirements?
Options:
A.Create a container for the job. Schedule the job to run as an AWS Fargate task on an Amazon Elastic Container Service (Amazon ECS) cluster by using Amazon EventBridge Scheduler.
B.Configure the job to run in an AWS Lambda function. Create a scheduled rule in Amazon EventBridge to invoke the Lambda function.
C.Configure an Auto Scaling group of Amazon EC2 Spot Instances that run Amazon Linux. Configure a crontab entry on the instances to run the analysis.
D.Configure an AWS DataSync task to run the job. Configure a cron expression to run the task on a schedule.
Answer: A
Explanation:

- A is correct because ECS + Fargate ensures no interruptions and easy scheduling.

- B is wrong because Lambda cannot handle long-running jobs.

- C is wrong because Spot Instances may interrupt.

- D is wrong because DataSync is for file transfer, not jobs.

Question 698:
A company runs workloads in the AWS Cloud. The company wants to centrally collect security data to assess security across the entire company and to improve workload protection. Which solution will meet these requirements with the LEAST development effort?
Options:
A.Configure a data lake in AWS Lake Formation. Use AWS Glue crawlers to ingest the security data into the data lake.
B.Configure an AWS Lambda function to collect the security data in .csv format. Upload the data to an Amazon S3 bucket.
C.Configure a data lake in Amazon Security Lake to collect the security data. Upload the data to an Amazon S3 bucket.
D.Configure an AWS Database Migration Service (AWS DMS) replication instance to load the security data into an Amazon RDS cluster.
Answer: C
Explanation:

- C is correct because Security Lake natively collects and normalizes security data.

- A is wrong because Lake Formation requires more setup.

- B is wrong because Lambda + S3 requires custom development.

- D is wrong because DMS is for DB migrations.

Question 699:
A company is migrating five on-premises applications to VPCs in the AWS Cloud. Each application is currently deployed in isolated virtual networks on premises and should be deployed similarly in the AWS Cloud. The applications need to reach a shared services VPC. All the applications must be able to communicate with each other. If the migration is successful, the company will repeat the migration process for more than 100 applications. Which solution will meet these requirements with the LEAST administrative overhead?
Options:
A.Deploy software VPN tunnels between the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets to the shared services VPC.
B.Deploy VPC peering connections between the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets to the shared services VPC through the peering connection.
C.Deploy an AWS Direct Connect connection between the application VPCs and the shared services VPC. Add routes from the application VPCs in their subnets to the shared services VPC and the applications VPCs. Add routes from the shared services VPC subnets to the applications VPCs.
D.Deploy a transit gateway with associations between the transit gateway and the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets and the application VPCs to the shared services VPC through the transit gateway.
Answer: D
Explanation:

- D is correct because a Transit Gateway scales well for 100+ VPCs.

- A is wrong because VPN tunnels do not scale.

- B is wrong because VPC peering does not scale beyond a few VPCs.

- C is wrong because Direct Connect is for on-premises, not intra-cloud VPCs.

Question 700:
A company wants to use Amazon Elastic Container Service (Amazon ECS) to run its on-premises application in a hybrid environment. The application currently runs on containers on premises. The company needs a single container solution that can scale in an on-premises, hybrid, or cloud environment. The company must run new application containers in the AWS Cloud and must use a load balancer for HTTP traffic. Which combination of actions will meet these requirements? (Choose two.)
Options:
A.Set up an ECS cluster that uses the AWS Fargate launch type for the cloud application containers. Use an Amazon ECS Anywhere external launch type for the on-premises application containers.
B.Set up an Application Load Balancer for cloud ECS services.
C.Set up a Network Load Balancer for cloud ECS services.
D.Set up an ECS cluster that uses the AWS Fargate launch type. Use Fargate for the cloud application containers and the on-premises application containers.
E.Set up an ECS cluster that uses the Amazon EC2 launch type for the cloud application containers. Use Amazon ECS Anywhere with an AWS Fargate launch type for the on-premises application containers.

Answer: AB
Explanation:

- A is correct because ECS Anywhere supports hybrid container environments.

- B is correct because ALB supports HTTP routing for ECS.

- C is wrong because NLB is for TCP/UDP, not HTTP.

- D is wrong because Fargate cannot run on-premises.

Question: 701
A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.
What should the solutions architect do to enable Internet access for the private subnets?

Options:
A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only Internet gateway.

Answer: A

Explanation:

- A: Correct. NAT gateways in each AZ provide fault tolerance and allow private subnets to reach the internet.

- B: Incorrect. NAT instances are older, less scalable, and require manual management.

- C: Incorrect. A VPC can only attach one internet gateway.

- D: Incorrect. Egress-only gateways are for IPv6, not IPv4.

Question: 702

A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system. Which combination of steps should a solutions architect take to automate this task? (Choose two.)

Options:

A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
B. Install an AWS DataSync agent in the on-premises data center.
C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
D. Manually use an operating system copy command to push the data to the EC2 instance.
E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

Answer: B, E

Explanation:

- A: Not needed for automation; EC2 placement is standard.

- B: Correct. DataSync agent enables automated secure transfer from on-premises.

- C: Incorrect. EBS is not required; target is EFS.

- D: Incorrect. Manual copy is not automated.

- E: Correct. Configuring DataSync location completes automation to EFS.

Question: 703

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

Options:

A. Edit the job to use job bookmarks.
B. Edit the job to delete data after the data is processed.
C. Edit the job by setting the NumberOfWorkers field to 1.
D. Use a FindMatches machine learning (ML) transform.

Answer: A

Explanation:

- A: Correct. Job bookmarks track processed data and avoid reprocessing.

- B: Incorrect. Deleting processed data may lose needed history.

- C: Incorrect. Worker count doesn't control reprocessing.

- D: Incorrect. ML transform is unrelated to this requirement.

Question: 704

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

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

Options:

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

B. Configure Amazon GuardDuty to automatically block the attackers.

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

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

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

Answer: A, C

Explanation:

- A: Correct. AWS Shield Advanced provides enhanced DDoS protection.

- B: Incorrect. GuardDuty detects threats, does not block traffic.

- C: Correct. CloudFront absorbs traffic at edge locations and improves resiliency.

- D: Incorrect. Lambda and ACLs are not scalable for massive DDoS.

- E: Incorrect. Spot Instances don't mitigate DDoS attacks.

Question: 705

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

Options:

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

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

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

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

Answer: D

Explanation:

- A: Incorrect. Too broad and violates least privilege.

- B: Incorrect. Execution role is not for EventBridge invoking.

- C: Incorrect. lambda:* is overly permissive.

- D: Correct. Resource-based policy with invoke permission allows EventBridge to trigger function.

Question: 706
A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year. Which solution meets these requirements and is the MOST operationally efficient?

Options:
A. Server-side encryption with customer-provided keys (SSE-C)
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
C. Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation
D. Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation

Answer: D

Explanation:

- A: Incorrect. SSE-C shifts key management burden to customer.

- B: Incorrect. SSE-S3 doesn't provide key usage logging or rotation.

- C: Incorrect. Manual rotation increases operational overhead.

- D: Correct. SSE-KMS with automatic rotation and CloudTrail logs satisfies compliance with least effort.

Question: 707
A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API. Which action meets these requirements for storing and retrieving location data?

Options:
A. Use Amazon Athena with Amazon S3.
B. Use Amazon API Gateway with AWS Lambda.
C. Use Amazon QuickSight with Amazon Redshift.
D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Answer: B

Explanation:

- A: Incorrect. Athena queries static data, not for real-time REST API.

- B: Correct. API Gateway + Lambda provides scalable REST API access to data.

- C: Incorrect. QuickSight is visualization, not a data store or API.

- D: Incorrect. Kinesis Data Analytics processes streams, not a REST API front-end.

Question: 708

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

Which design should a solutions architect recommend?

Options:

A. Create an AWS Lambda function triggered when the RDS database is updated to send the information to an Amazon SQS queue for the targets to consume.

B. Create an AWS Lambda function triggered when the RDS database is updated to send the information to an Amazon SQS FIFO queue for the targets to consume.

C. Subscribe to an RDS event notification and send an SQS queue fanned out to multiple SNS topics. Use Lambda functions to update the targets.

D. Subscribe to an RDS event notification and send an SNS topic fanned out to multiple SQS queues. Use Lambda functions to update the targets.

Answer: D

Explanation:

- A: Incorrect. SQS fanout to multiple systems is missing.

- B: Incorrect. FIFO is unnecessary here.

- C: Incorrect. RDS events to SQS then SNS is backwards.

- D: Correct. RDS events → SNS → SQS fanout → Lambda ensures reliable multi-target delivery.

Question: 709

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

What should a solutions architect do to meet these requirements?

Options:

A. Create an S3 Glacier vault. Apply a WORM vault lock policy to the objects.

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

C. Create an S3 bucket. Use CloudTrail to track modifications and restore objects from backups if needed.

D. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add s3:PutObjectLegalHold to IAM policies for delete permissions.

Answer: D

Explanation:

- A: Incorrect. Glacier Vault Lock works, but S3 Object Lock is better for fine-grained control.

- B: Incorrect. Fixed retention doesn't provide flexibility for indefinite hold.

- C: Incorrect. Detect-and-restore is reactive, not prevention.

- D: Correct. Object Lock with legal hold provides compliance and selective delete control.

Question: 710

A social media company allows users to upload images. The website runs on EC2 instances. During upload requests, the website resizes the images and stores them in Amazon S3. Users report slow uploads. The company needs to reduce coupling and improve performance with minimal operations.

Which combination should the solutions architect recommend? (Choose two.)

Options:

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

B. Configure the web server to upload the original images to Amazon S3.

C. Configure the application to upload images directly from each user's browser to S3 using presigned URLs.

D. Configure S3 Event Notifications to trigger a Lambda function that resizes the image.

E. Create an EventBridge rule that invokes a Lambda function on a schedule to resize images.

Answer: B, D

Explanation:

- A: Incorrect. Glacier is archival, not for active image storage.

- B: Correct. Upload originals directly to S3.

- C: Incorrect in this scenario since resizing requires post-processing.

- D: Correct. Lambda + S3 Event decouples processing from upload.

- E: Incorrect. Scheduled resize delays processing.

Question: 713

A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center does not have any available network bandwidth for additional workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.

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

Options:

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

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

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

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

Answer: C

Explanation:

- A: Incorrect. DataSync requires network bandwidth, which is unavailable.

- B: Incorrect. Snowcone has limited storage, not sufficient for 50 TB.

- C: Correct. Snowball Edge Storage Optimized device handles 50 TB, AWS Glue for transformations minimizes ops.

- D: Incorrect. Extra step of provisioning EC2 to run transformations increases overhead.

Question: 714

A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meats these requirements?

Options:

A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Answer: C

Explanation:

- A: Incorrect. Storing photos in DynamoDB is not efficient or cost-effective.

- B: Incorrect. Kinesis Firehose is for streaming data ingestion, not image processing.

- C: Correct. Lambda scales automatically, S3 is best for photo storage, DynamoDB remains for metadata.

- D: Incorrect. Scaling to 3 EC2s is not elastic and doesn't handle sudden spikes well.

Question: 715

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

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

Options:

A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.
D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer: C

Explanation:

- A: Incorrect. NAT still sends traffic through the internet.

- B: Incorrect. Security groups alone don't change the route path, traffic still goes public.

- C: Correct. VPC Gateway Endpoint ensures private connection to S3 with no internet traversal.

- D: Incorrect. Direct Connect is unnecessary for simple private S3 connectivity.

Question: 716

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

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

Options:
A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.
B. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.
C. Create and deploy an AWS Lambda function to manage and serve the website content.
D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
E. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Answer: AD

Explanation:

- A: Correct. CloudFront improves security (HTTPS, DDoS protection) and performance.

- B: Incorrect. WAF protects but does not reduce ops overhead like CloudFront.

- C: Incorrect. Lambda for hosting website adds unnecessary complexity.

- D: Correct. S3 static website hosting is cost-effective, simple, highly scalable.

- E: Incorrect. EC2 + ALB adds management overhead, unnecessary for static content.

Question: 717

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

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

Options:

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

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

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

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

Answer: A

Explanation:

- A: Correct. CloudWatch Logs subscription directly streams logs to OpenSearch with minimal setup.

- B: Incorrect. Lambda adds unnecessary operational overhead.

- C: Incorrect. Kinesis Firehose adds extra step; not the simplest solution.

- D: Incorrect. Kinesis Agent + Streams adds more complexity than needed.

Question: 718

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

Which storage solution meets these requirements MOST cost-effectively?

Options:

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon OpenSearch Service (Amazon Elasticsearch Service)
D. Amazon S3

Answer: D

Explanation:

- A: Incorrect. EBS cannot scale to 900 TB easily, tied to EC2.

- B: Incorrect. EFS is more expensive and unnecessary for simple document storage.

- C: Incorrect. OpenSearch is not for storing 900 TB of text documents.

- D: Correct. S3 scales virtually infinitely, cost-effective, highly durable.

Question: 719

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

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

Options:

A. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.
B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.
C. Set up AWS Shield in bath Regions. Associate Regional web ACLs with an API stage.
D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

Answer: B

Explanation:

- A: Incorrect. Requires manual setup per Region/account.

- B: Correct. Firewall Manager centralizes WAF rule management across Regions/accounts.

- C: Incorrect. AWS Shield is for DDoS, not SQL injection/XSS.

- D: Incorrect. Same issue, plus wrong security tool.

Question: 720

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

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

Options:

A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.
C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Answer: B

Explanation:

- A: Incorrect. CloudFront with geolocation adds complexity, not optimal for DNS performance.

- B: Correct. Global Accelerator provides improved latency, health checks, and routes to NLB endpoints.

- C: Incorrect. Attaching EIPs to instances defeats load balancing and HA.

- D: Incorrect. Latency routing via ALB + CloudFront is possible but more complex than Global Accelerator.

Question: 721

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.
What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

Options:
A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance.
D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Answer: A

Explanation:

- A: Correct. RDS encryption can only be enabled at creation/restore. Must restore from encrypted snapshot.

- B: Incorrect. Cannot just attach encrypted EBS volume to RDS.

- C: Incorrect. Cannot restore encrypted snapshot to existing unencrypted instance. Must create new encrypted instance.

- D: Incorrect. Copying snapshots to S3 does not solve RDS encryption requirement.

Question: 722

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.
What should a solutions architect do to reduce the operational burden?

Options:
A. Use multi-factor authentication (MFA) to protect the encryption keys.
B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Answer: B

Explanation:

- A: Incorrect. MFA protects accounts, not scalable encryption key management.

- B: Correct. AWS KMS manages encryption keys, integrates with AWS services, minimizes overhead.

- C: Incorrect. ACM is for SSL/TLS certificates, not data encryption keys.

- D: Incorrect. IAM policies alone don't manage keys.

Question: 723

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

What should a solutions architect do to increase the application's performance?

Options:

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

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

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

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

Answer: D

Explanation:

- A: Incorrect. ACM certs don't terminate SSL directly on EC2, just simplifies cert management.

- B: Incorrect. S3 cannot terminate SSL.

- C: Incorrect. Adds more infra and bottlenecks.

- D: Correct. Offloading SSL to ALB improves performance and scalability.

Question: 724

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

What should the solutions architect recommend?

Options:

A. Implement EC2 Spot Instances.

B. Purchase EC2 Reserved Instances.

C. Implement EC2 On-Demand Instances.

D. Implement the processing on AWS Lambda.

Answer: A

Explanation:

- A: Correct. Spot Instances are cheap, scalable, and suitable for interruptible, stateless workloads.

- B: Incorrect. Reserved Instances are for steady-state predictable workloads, not dynamic jobs.

- C: Incorrect. On-Demand is flexible but costly compared to Spot for this use case.

- D: Incorrect. Lambda cannot handle long-running batch jobs exceeding 15 minutes.

Question: 725

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

Options:
A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Answer: AE

Explanation:

- A: Correct. EC2 and RDS in private subnets secure the app; Multi-AZ RDS ensures HA.

- B: Incorrect. ALB must be in public subnets to serve traffic.

- C: Incorrect. Placing EC2 in public subnets exposes them to the internet.

- D: Incorrect. Only one public subnet is insufficient for HA.

- E: Correct. Public subnets host ALB; private subnets host EC2 + RDS; NAT gateways provide internet access.

Question: 726
A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.
Which solution will meet these requirements?

Options:
A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

Answer: B

Explanation:

- A: Incorrect. Glacier Deep Archive cannot meet immediate retrieval requirement for first 2 years.

- B: Correct. Keep 2 years in S3 Standard; archive older data cost-effectively in Deep Archive.

- C: Incorrect. Intelligent-Tiering does not guarantee long-term archival compliance.

- D: Incorrect. One Zone-IA reduces availability, not required here.

Question: 727
A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.
Which set of services should a solutions architect recommend to meet these requirements?

Options:
A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Answer: D

Explanation:

- A: Incorrect. EBS is durable but not optimal for 10 TB max-performance processing. Instance store is faster.

- B: Incorrect. EFS is expensive for 300 TB storage.

- C: Incorrect. EFS for durable storage is unnecessary; S3 is better suited.

- D: Correct. EC2 instance store = high I/O, S3 = durable media storage, Glacier = ~~archival.~~

Question: 728
A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.
What should a solutions architect do to meet these requirements?

Options:
A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Answer: B

Explanation:

- A: Incorrect. EC2 + Spot needs manual container orchestration, higher ops overhead.

- B: Correct. EKS managed node groups + Spot minimize ops while reducing cost.

- C: Incorrect. On-Demand is costly compared to Spot.

- D: Incorrect. On-Demand increases cost unnecessarily.

Question: 729
A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.
Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

Options:
A. Migrate the PostgreSQL database to Amazon Aurora.
B. Migrate the web application to be hosted on Amazon EC2 instances.
C. Set up an Amazon CloudFront distribution for the web application content.
D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer: AE

Explanation:

- A: Correct. Aurora is fully managed, reduces DB ops overhead.

- B: Incorrect. EC2 still requires capacity and infra management.

- C: Incorrect. CloudFront does not address infra and scaling needs here.

- D: Incorrect. ElastiCache improves performance, but does not address ops burden.

- E: Correct. Fargate removes need to manage servers, scales containers easily.

Question: 730
An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.
What should a solutions architect do to maintain the desired performance across all instances in the group?

Options:
A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
B. Use a target tracking policy to dynamically scale the Auto Scaling group.
C. Use an AWS Lambda function ta update the desired Auto Scaling group capacity.
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Answer: B

Explanation:

- A: Incorrect. Simple scaling reacts only to thresholds, not target utilization.

- B: Correct. Target tracking maintains CPU utilization close to 40% automatically.

- C: Incorrect. Lambda custom scaling adds unnecessary complexity.

- D: Incorrect. Scheduled scaling doesn't handle variable CPU patterns.

Question: 731
A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL. What should a solutions architect do to meet these requirements?

Options:
A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Answer: D

Explanation:

- A: Incorrect. Not scalable, high management overhead.

- B: Incorrect. IAM users cannot be directly assigned to CloudFront.

- C: Incorrect. CloudFront does not use distribution ID as a Principal in bucket policy.

- D: Correct. OAI restricts access so only CloudFront can read S3 objects.

Question: 732
A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.
Which combination should a solutions architect recommend to meet these requirements?

Options:
A. Amazon CloudFront and Amazon S3
B. AWS Lambda and Amazon DynamoDB
C. Application Load Balancer with Amazon EC2 Auto Scaling
D. Amazon Route 53 with internal Application Load Balancers

Answer: A

Explanation:

- A: Correct. CloudFront + S3 provides global scale, cost efficiency, and fast response.

- B: Incorrect. Lambda + DynamoDB is serverless compute and DB, not for static file distribution.

- C: Incorrect. ALB + EC2 scaling adds unnecessary cost and ops.

- D: Incorrect. Route 53 + ALBs doesn't solve performance and cost optimization for downloads.

Question: 733
A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.
Which solution will meet these requirements?

Options:
A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.
D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Answer: C

Explanation:

- A: Incorrect. EC2 increases ops burden to manage replication and OS.

- B: Incorrect. Automated backups don't provide real-time DR.

- C: Correct. RDS Custom for Oracle gives OS access and supports read replica for DR.

- D: Incorrect. Multi-AZ only provides HA, not DR across Regions.

Question: 734

A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region. Which solution will meet these requirements with the LEAST operational overhead?

Options:

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

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

C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.

D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

Answer: A

Explanation:

- A: Correct. SSE-KMS multi-Region keys ensure encryption + replication, Athena queries serverlessly.

- B: Incorrect. RDS adds unnecessary ops burden for queries.

- C: Incorrect. SSE-S3 doesn't support KMS-level audit/rotation requirements.

- D: Incorrect. Same as C, plus RDS overhead.

Question: 735

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

Options:

A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.

B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.

C. Create a NAT gateway in a public subnet of the company's VPUpdate the route table to connect to the target service.

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

Answer: D

Explanation:

- A: Incorrect. VPC peering exposes full network ranges, not just service.

- B: Incorrect. Virtual private gateway is for VPN/Direct Connect, not service-specific.

- C: Incorrect. NAT gateway routes traffic via internet, not private.

- D: Correct. PrivateLink restricts access to the provider service privately and securely.

Question: 736
A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.
Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

Options:
A. Create an ongoing replication task.
B. Create a database backup of the on-premises database.
C. Create an AWS Database Migration Service (AWS DMS) replication server.
D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

Answer: AC

Explanation:

- A: Correct. Ongoing replication task keeps databases in sync.

- B: Incorrect. Backup alone doesn't support live sync.

- C: Correct. DMS replication server is required for migration and sync.

- D: Incorrect. SCT only needed if schema conversion required (same engine here).

- E: Incorrect. EventBridge not required for synchronization.

Question: 737
A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators.
Which solution will meet these requirements?

Options:
A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.

D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Answer: B

Explanation:

- A: Incorrect. Forwards to all users, not limited to admins.

- B: Correct. Distribution list + alternate contacts ensures only admins get notifications.

- C: Incorrect. Single point of failure with one admin.

- D: Incorrect. Same root email across accounts reduces security and traceability.

Question: 738
A company runs its ecommerce application on AWS. Every new order is published as a massage in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone.
The company needs to redesign its architecture to provide the highest availability with the least operational overhead.
What should a solutions architect do to meet these requirements?

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

Answer: B

Explanation:

- A: Incorrect. Database on EC2 lacks managed HA; higher ops overhead.

- B: Correct. Amazon MQ + RDS Multi-AZ + Auto Scaling consumers provides HA and reduces ops burden.

- C: Incorrect. Self-managing RabbitMQ on EC2 increases complexity.

- D: Incorrect. EC2-based DB management is not recommended.

Question: 739

A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

Options:

A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.

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

C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.

D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Answer: D

Explanation:

- A: Incorrect. Manual Lambda copy adds ops overhead.

- B: Incorrect. Same as A, still relies on custom Lambda for copying.

- C: Incorrect. Using replication is correct, but event notifications tied incorrectly.

- D: Correct. S3 replication automates copying + EventBridge triggers Lambda and SageMaker.

Question: 740

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year. Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

Options:

A. Use Spot Instances for the data ingestion layer

B. Use On-Demand Instances for the data ingestion layer

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

D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.

E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Answer: AC

Explanation:

- A: Correct. Spot Instances fit sporadic, interruptible workloads.

- B: Incorrect. On-Demand is more expensive for unpredictable workloads.

- C: Correct. Compute Savings Plan reduces cost for predictable Fargate + Lambda usage.

- D: Incorrect. Reserved Instances not suited for sporadic EC2 ingestion workloads.

- E: Incorrect. Instance Savings Plan does not apply to Fargate + Lambda.

Question: 741

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

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

Options:

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

B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.

C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.

D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Answer: A

Explanation:

- A: Correct. CloudFront accelerates both static + dynamic content globally using ALB as origin.

- B: Incorrect. Multi-Region increases ops burden and cost.

- C: Incorrect. Serving dynamic content directly adds latency.

- D: Incorrect. Geo-routing adds complexity and cost without CloudFront acceleration.

Question: 742

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

What should a solutions architect do to meet these requirements?

Options:

A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.

B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.

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

D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Answer: C

Explanation:

- A: Incorrect. Route 53 only provides DNS resolution, not static IPs.

- B: Incorrect. CloudFront doesn't support UDP-based workloads.

- C: Correct. Global Accelerator provides static IPs, routes to nearest edge location, supports UDP.

- D: Incorrect. API Gateway is HTTP-based, not for UDP workloads.

Question: 743

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

Which solution will meet these requirements?

Options:

A. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.

B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.

C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.

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

Answer: D

Explanation:

- A: Incorrect. Requires rewriting monolithic app into Lambda functions.

- B: Incorrect. Amplify is for frontend apps, not backend microservices.

- C: Incorrect. EC2 scaling adds ops overhead.

- D: Correct. ECS allows microservices split, managed separately, scalable, less ops overhead.

Question: 744

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

What is the MOST cost-effective solution?

Options:

A. Migrate the monthly reporting to Amazon Redshift.

B. Migrate the monthly reporting to an Aurora Replica.

C. Migrate the Aurora database to a larger instance class.

D. Increase the Provisioned IOPS on the Aurora instance.

Answer: B

Explanation:

- A: Incorrect. Redshift is powerful but unnecessary for this use case.

- B: Correct. Aurora Replicas offload read traffic, cost-effective solution.

- C: Incorrect. Scaling up instance increases cost unnecessarily.

- D: Incorrect. Provisioned IOPS helps only if I/O is the bottleneck; CPU also high.

Question: 745

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

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

Answer: D

Explanation:

- A: Incorrect. Only two EC2 instances, no Auto Scaling for seamless scale.

- B: Incorrect. Route 53 weighted routing doesn't handle auto scaling.

- C: Incorrect. Manual resizing with Lambda is reactive, not seamless.

- D: Correct. Aurora + Auto Scaling + ALB with Spot Fleet is cost-effective and scalable.

Question: 746

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

Options:
A. Use Spot Instances for the entire workload.
B. Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs.
C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.

Answer: B

Explanation:

- A: Incorrect. Spot alone risks interruptions for production workloads.

- B: Correct. Reserved for baseline steady usage + Spot for burst = cost optimized.

- C: Incorrect. On-Demand for baseline is costlier than Reserved.

- D: Incorrect. Dedicated Instances unnecessary and expensive.

Question: 747

A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.

Which storage option meets these requirements MOST cost-effectively?

Options:

A. Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

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

C. Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

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

Answer: B

Explanation:

- A: Incorrect. AWS Backup not required; S3 Lifecycle is simpler.

- B: Correct. S3 Lifecycle to Deep Archive minimizes cost for long retention.

- C: Incorrect. CloudWatch Logs storage not cost-effective for TBs of data.

- D: Incorrect. Lifecycle cannot be applied directly on CloudWatch Logs.

Question: 748

A company has a data ingestion workflow that includes the following components:

- An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries

- An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues. When failure occurs, the corresponding data is not ingested unless the company manually reruns the job.

What should a solutions architect do to ensure that all notifications are eventually processed?

Options:

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

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

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

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

Answer: D

Explanation:

- A: Incorrect. Lambda is already AZ-resilient.

- B: Incorrect. More CPU/memory doesn't solve network issues.

- C: Incorrect. Retries alone risk message loss if failures persist.

- D: Correct. SQS as DLQ ensures messages persist until processed.

Question: 749
A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.
How should a solutions architect accomplish this?

Options:
A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer: A

Explanation:

- A: Correct. FIFO queue preserves order, Lambda serverlessly processes events.

- B: Incorrect. SNS doesn't guarantee ordering.

- C: Incorrect. Standard SQS doesn't preserve ordering.

- D: Incorrect. SNS + SQS combo still doesn't guarantee strict ordering.

Question: 750

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

What should the solutions architect do to meet these requirements?

Options:

A. Create Amazon CloudWatch composite alarms where possible.

B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.

C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.

D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Answer: A

Explanation:

- A: Correct. Composite alarms combine multiple conditions, reducing false alarms.

- B: Incorrect. Dashboards are monitoring tools, not proactive alarms.

- C: Incorrect. Canaries simulate transactions, not infra metric correlation.

- D: Incorrect. Single alarms cannot check multiple metrics together.

Question: 751

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

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

Options:

A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.

B. Use rules in AWS WAF to prevent internet access. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.

C. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.

D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.

E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Answer: AC

Explanation:

- A: Correct. Control Tower guardrails can enforce region restriction and deny internet gateways.

- B: Incorrect. WAF is for HTTP/HTTPS traffic filtering, not VPC internet access control.

- C: Correct. SCPs prevent unwanted actions across accounts, including blocking internet gateways and region usage.

- D: Incorrect. NACLs + IAM don't enforce full compliance consistently across all accounts.

- E: Incorrect. AWS Config detects violations but does not prevent them.

Question: 752
A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.
What should a solutions architect do to meet these requirements?

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

Answer: D

Explanation:

- A: Incorrect. Systems Manager is not needed for scheduling start/stop of RDS.

- B: Incorrect. ElastiCache cannot replace a stopped DB instance.

- C: Incorrect. EC2 instance cron jobs add unnecessary ops overhead.

- D: Correct. Lambda + EventBridge can schedule start/stop with minimal cost and ops.

Question: 753
A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.
Which action should the company take to meet these requirements MOST cost-effectively?

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

Answer: D

Explanation:

- A: Incorrect. Storing everything initially in IA is more expensive for frequent access.

- B: Incorrect. Intelligent-Tiering incurs extra monitoring fees; lifecycle policy is cheaper here.

- C: Incorrect. Inventory is for reporting, not lifecycle transitions.

- D: Correct. Lifecycle transitions to S3 Standard-IA after 90 days is the most cost-effective.

Question: 754
A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.
Which solution will meet these requirements?

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

Answer: B

Explanation:

- A: Incorrect. Governance mode allows privileged users to override retention.

- B: Correct. Compliance mode ensures immutability for 365 days with no bypass.

- C: Incorrect. IAM/bucket policies cannot enforce WORM compliance.

- D: Incorrect. Lambda cannot guarantee prevention of modification/deletion.

Question: 755

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

Which solution will meet these requirements?

Options:

A. Use AWS DataSync to connect the S3 buckets to the web application.

B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.

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

D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Answer: C

Explanation:

- A: Incorrect. DataSync is for data transfers, not global content delivery.

- B: Incorrect. Global Accelerator improves routing, not caching media globally.

- C: Correct. CloudFront caches and delivers S3 content worldwide.

- D: Incorrect. SQS is a messaging service, irrelevant to content caching.

Question: 756

A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

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

Options:

A. Use Amazon Athena for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.

B. Use Amazon Kinesis Data Analytics for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.

C. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster.

D. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format. Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters.

E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load the data into Amazon S3 in Apache Parquet format.

Answer: AE

Explanation:

- A: Correct. Athena queries S3 directly, QuickSight dashboards BI easily.

- B: Incorrect. Kinesis Data Analytics is for real-time queries, not one-time.

- C: Incorrect. Custom Lambda adds ops burden and complexity.

- D: Incorrect. OpenSearch is not suitable for BI analytics, unnecessary overhead.

- E: Correct. Lake Formation + Glue simplifies ingest and Parquet staging for analytics.

Question: 757
A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

Options:
A. Take a manual snapshot of the DB cluster.
B. Create a lifecycle policy for the automated backups.
C. Configure automated backup retention for 5 years.
D. Configure an Amazon CloudWatch Logs export for the DB cluster.
E. Use AWS Backup to take the backups and to keep the backups for 5 years.

Answer: DE

Explanation:

- A: Incorrect. Manual snapshots don't enforce lifecycle automatically.

- B: Incorrect. Aurora automated backup retention cannot go up to 5 years.

- C: Incorrect. Aurora supports max 35 days retention.

- D: Correct. Logs must be exported to CloudWatch Logs for indefinite retention.

- E: Correct. AWS Backup can manage 5-year retention with policies.

Question: 758
A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.
Which service will improve the performance of both the real-time and on-demand streaming?

Options:
A. Amazon CloudFront
B. AWS Global Accelerator
C. Amazon Route 53
D. Amazon S3 Transfer Acceleration

Answer: A

Explanation:

- A: Correct. CloudFront supports live streaming and on-demand video globally.

- B: Incorrect. Global Accelerator improves routing but not streaming performance.

- C: Incorrect. Route 53 is DNS-based routing, not streaming optimization.

- D: Incorrect. S3 Transfer Acceleration is for uploads, not media delivery.

Question: 759
A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.
Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

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

Answer: AC

Explanation:

- A: Correct. API keys restrict access to authorized users only.

- B: Incorrect. Adding logic in Lambda increases latency and ops effort.

- C: Correct. WAF blocks malicious requests before they reach API Gateway.

- D: Incorrect. Making it private would block genuine public users.

- E: Incorrect. IAM roles are not scalable for millions of API consumers.

Question: 760
An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.
Which solution meets these requirements MOST cost-effectively?

Options:
A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
B. Amazon S3 Glacier
C. Amazon S3 Standard
D. Amazon RDS for PostgreSQL

Answer: C

Explanation:

- A: Incorrect. OpenSearch is for search/analytics, not backup.

- B: Incorrect. S3 Glacier retrieval takes minutes/hours, not milliseconds.

- C: Correct. S3 Standard provides millisecond access and is cost-effective for 30 days.

- D: Incorrect. RDS is for relational workloads, not JSON storage backup.

Question: 761
A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.
Which solution will meet these requirements?

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

Answer: B

Explanation:

- A: Incorrect. EC2 requires management and scaling overhead.

- B: Correct. Lambda + S3 event triggers scale automatically with no servers.

- C: Incorrect. EBS Multi-Attach doesn't fit; high ops overhead.

- D: Incorrect. ECS with EC2 adds ops burden compared to serverless Lambda.

Question: 762

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

Which combination of AWS services meets these requirements?

Options:

A. Amazon FSx for Lustre integrated with Amazon S3
B. Amazon FSx for Windows File Server integrated with Amazon S3
C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Answer: A

Explanation:

- A: Correct. FSx for Lustre is built for HPC and integrates with S3.

- B: Incorrect. FSx for Windows is for Windows workloads, not HPC.

- C: Incorrect. Glacier is archive storage, not HPC-optimized.

- D: Incorrect. S3 + EBS is not integrated as a high-performance HPC file system.

Question: 763

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

Which solution will meet these requirements?

Options:

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

Answer: A

Explanation:

- A: Correct. ECS with Fargate is fully managed, scales automatically, minimal ops.

- B: Incorrect. ECS with EC2 requires EC2 management overhead.

- C: Incorrect. Self-managed repo/EC2 increases ops complexity.

- D: Incorrect. Running containers as AMIs on EC2 removes container benefits.

Question: 764

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

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

Answer: C

Explanation:

- A: Incorrect. Redis on EC2 is not durable or managed, adds ops.

- B: Incorrect. Kinesis is more complex and unnecessary for low-volume 1,000/hr messages.

- C: Correct. SQS with DLQ ensures durability, retries, and retention with low ops.

- D: Incorrect. SNS doesn't support message retention/replay.

Question: 765

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

Options:
A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.

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

Answer: D

Explanation:

- A: Incorrect. S3 bucket policies cannot filter by WAF ARN.

- B: Incorrect. WAF integrates with CloudFront, not S3 directly.

- C: Incorrect. Security groups don't apply to S3 buckets.

- D: Correct. OAI restricts direct S3 access; WAF inspects all CloudFront traffic.

Question: 766
Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.
Which action should the solutions architect take to accomplish this?

Options:
A. Generate presigned URLs for the files.
B. Use cross-Region replication to all Regions.
C. Use the geoproximity feature of Amazon Route 53.
D. Use Amazon CloudFront with the S3 bucket as its origin.

Answer: D

Explanation:

- A: Incorrect. Presigned URLs are for restricted access, not global distribution.

- B: Incorrect. Cross-Region replication adds cost and doesn't solve latency.

- C: Incorrect. Route 53 only resolves DNS, doesn't cache content.

- D: Correct. CloudFront caches static S3 content globally at edge locations.

Question: 767
A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.
Which solution meets these requirements MOST cost-effectively?

Options:
A. Use Spot Instances exclusively to handle the maximum capacity required.
B. Use Reserved Instances exclusively to handle the maximum capacity required.
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Answer: D

Explanation:

- A: Incorrect. Spot-only risks interruptions, not reliable for continuous processing.

- B: Incorrect. Reserved-only is expensive and doesn't match unpredictable workloads.

- C: Incorrect. Spot is cheaper but not guaranteed; downtime may occur.

- D: Correct. Reserved covers baseline, On-Demand covers unpredictable spikes.

Question: 768
A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.
What should a solutions architect do to accomplish this?

Options:
A. Create an ACL to provide access to the services or actions.
B. Create a security group to allow accounts and attach it to user groups.
C. Create cross-account roles in each account to deny access to the services or actions.
D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

Explanation:

- A: Incorrect. ACLs are for networking, not IAM or service-level control.

- B: Incorrect. Security groups apply to resources, not AWS accounts.

- C: Incorrect. Cross-account roles are complex and not centralized.

- D: Correct. SCPs in Organizations centrally enforce restrictions across accounts.

Question: 769
A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.
What should the solutions architect do to meet this requirement?

Options:
A. Add an Amazon Inspector agent to the ALB.
B. Configure Amazon Macie to prevent attacks.
C. Enable AWS Shield Advanced to prevent attacks.
D. Configure Amazon GuardDuty to monitor the ALB.

Answer: C

Explanation:

- A: Incorrect. Inspector is for vulnerability assessment, not DDoS protection.

- B: Incorrect. Macie protects sensitive data, not against DDoS.

- C: Correct. Shield Advanced protects ALB from large-scale DDoS attacks.

- D: Incorrect. GuardDuty detects threats but doesn't prevent attacks.

Question: 770
A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.
Which configuration will meet this requirement?

Options:
A. Configure the security group for the EC2 instances.
B. Configure the security group on the Application Load Balancer.
C. Configure AWS WAF on the Application Load Balancer in a VPC.
D. Configure the network ACL for the subnet that contains the EC2 instances.

Answer: C

Explanation:

- A: Incorrect. Security groups don't support geolocation rules.

- B: Incorrect. Same limitation as instance-level SG.

- C: Correct. WAF supports geolocation filtering at the ALB layer.

- D: Incorrect. NACLs allow IP-based rules, but not by country.

Question: 771
A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.
What should the solutions architect do to accomplish this?

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

Answer: B

Explanation:

- A: Incorrect. Single EC2 instance cannot scale elastically.

- B: Correct. API Gateway + Lambda scales automatically with demand.

- C: Incorrect. Two EC2 instances are not elastic enough for large spikes.

- D: Incorrect. EC2 backend still limits scalability.

Question: 772

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

Options:

A. Configure a CloudFront signed URL.

B. Configure a CloudFront signed cookie.

C. Configure a CloudFront field-level encryption profile.

D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Answer: C

Explanation:

- A: Incorrect. Signed URLs restrict access, not encryption of fields.

- B: Incorrect. Signed cookies are for access control, not field-level protection.

- C: Correct. Field-level encryption secures sensitive data end-to-end.

- D: Incorrect. HTTPS-only ensures transport security but doesn't encrypt specific fields.

Question: 773

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

Options:

A. Deploy an AWS Global Accelerator accelerator in front of the web servers.

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

C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.

D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Answer: B

Explanation:

- A: Incorrect. Global Accelerator helps routing, not caching content.

- B: Correct. CloudFront caches and distributes S3 content globally at scale.

- C: Incorrect. Redis is for app-level caching, not global media distribution.

- D: Incorrect. Memcached is for in-memory caching, not suitable for this case.

Question: 774

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

Which architecture should the solutions architect choose that provides high availability?

Options:

A. Create an Auto Scaling group that uses three instances across each of two Regions.

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

C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.

D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

Explanation:

- A: Incorrect. Multi-Region isn't needed here.

- B: Correct. High availability comes from distributing EC2 instances across multiple AZs.

- C: Incorrect. A template doesn't automatically ensure HA.

- D: Incorrect. ALB already balances traffic, but across one AZ only.

Question: 775

An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts, and the application did not process the orders of those customers.

A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

Options:

A. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.

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

C. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.

D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

Answer: B

Explanation:

- A: Incorrect. Provisioned concurrency helps Lambda but doesn't solve DB connections.

- B: Correct. RDS Proxy pools and reuses connections, reducing database load.

- C: Incorrect. Read replicas don't reduce write connection load and Region adds latency.

- D: Incorrect. DynamoDB migration is unnecessary and major refactor.

Question: 776
An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.
What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

Options:
A. Use a VPC endpoint for DynamoDB.
B. Use a NAT gateway in a public subnet.
C. Use a NAT instance in a private subnet.
D. Use the internet gateway attached to the VPC.

Answer: A

Explanation:

- A: Correct. VPC endpoints enable private connectivity without internet.

- B: Incorrect. NAT sends traffic over internet path.

- C: Incorrect. Same as NAT gateway, still uses internet path.

- D: Incorrect. Direct internet is not secure and breaks requirements.

Question: 777
An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.
What should a solutions architect recommend to meet this requirement?

Options:
A. Use Amazon ElastiCache for Redis.
B. Use Amazon DynamoDB Accelerator (DAX).
C. Replicate data by using DynamoDB global tables.
D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Answer: B

Explanation:

- A: Incorrect. ElastiCache requires custom caching logic.

- B: Correct. DAX is a fully managed in-memory cache for DynamoDB with no app changes.

- C: Incorrect. Global tables are for multi-Region, not performance in same Region.

- D: Incorrect. Memcached also needs app reconfiguration.

Question: 778
A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.
B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.
C. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.
D. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.

Answer: A

Explanation:

- A: Correct. AWS Backup centrally manages cross-Region backups with minimal effort.

- B: Incorrect. DLM only supports EBS, not RDS.

- C: Incorrect. Manual AMIs and replicas require ongoing management.

- D: Incorrect. Too many manual steps and complexity.

Question: 779
A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.
What should the solutions architect do to meet this requirement?

Options:
A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.
B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.
C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.
D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

Answer: A

Explanation:

- A: Correct. IAM role + KMS decrypt + Parameter Store = secure access.

- B: Incorrect. EC2 instances can't directly assume IAM policies; needs a role.

- C: Incorrect. No trust relationships exist with Parameter Store.

- D: Incorrect. Trust between DB and EC2 is not valid.

Question: 780
A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.
Which combination of solutions provides the MOST protection? (Choose two.)

Options:
A. Use AWS WAF to protect the NLB.
B. Use AWS Shield Advanced with the NLB.
C. Use AWS WAF to protect Amazon API Gateway.
D. Use Amazon GuardDuty with AWS Shield Standard.
E. Use AWS Shield Standard with Amazon API Gateway.

Answer: BC

Explanation:

- A: Incorrect. WAF cannot be attached directly to NLB.

- B: Correct. Shield Advanced protects against DDoS at NLB.

- C: Correct. WAF protects API Gateway from SQL injection and XSS.

- D: Incorrect. GuardDuty detects but doesn't prevent.

- E: Incorrect. Shield Standard is always on but basic, not enough.

Question: 781
A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.
The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).
What should a solutions architect recommend for communication between the microservices?

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

Answer: A

Explanation:

- A: Correct. SQS decouples microservices and ensures scalability.

- B: Incorrect. SNS is push-based, not good for sequential processing.

- C: Incorrect. Lambda relay adds unnecessary overhead.

- D: Incorrect. DynamoDB Streams not needed for inter-service comms.

Question: 782
A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.
Which solution meets these requirements?

Options:
A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B

Explanation:

- A: Incorrect. RDS does not replicate to 3 nodes directly.

- B: Correct. Multi-AZ ensures synchronous replication for HA and durability.

- C: Incorrect. Cross-Region replication is asynchronous, not synchronous.

- D: Incorrect. Manual Lambda solution is complex and unreliable.

Question: 783
A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.
Which solution will meet these requirements?

Options:
A. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content.
B. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon Aurora with Aurora Auto Scaling for the database. Configure Amazon CloudFront to deliver the website content.
C. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon DynamoDB with provisioned write capacity for the database.
D. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon Aurora with Aurora Auto Scaling for the database.

Answer: A

Explanation:

- A: Correct. S3 + API Gateway + Lambda + DynamoDB (on-demand) = serverless, scalable, minimal ops.

- B: Incorrect. Aurora adds more ops overhead than DynamoDB.

- C: Incorrect. EC2 increases maintenance burden.

- D: Incorrect. Still EC2-based and not serverless.

Question: 784

A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

Options:

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

B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.

C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.

D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Answer: A

Explanation:

- A: Correct. Placing Lambda in VPC with the right SG allows secure access to the DB.

- B: Incorrect. A VPN is not needed since Direct Connect already exists.

- C: Incorrect. Routing doesn't work unless Lambda is in the VPC.

- D: Incorrect. Lambda doesn't use Elastic IPs directly.

Question: 785

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

Options:

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.

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

C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.

D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

Explanation:

- A: Incorrect. There is no "S3 role" in IAM. Needs ECS task role.

- B: Correct. Assigning a task role with S3 access is best practice.

- C: Incorrect. Security groups don't apply to S3 access.

- D: Incorrect. IAM user login is not scalable or secure.

Question: 786

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.

What should a solutions architect do to meet this requirement?

Options:

A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.

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

C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.

D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Answer: B

Explanation:

- A: Incorrect. Storage Gateway is for hybrid storage, not native shared FS.

- B: Correct. FSx for Windows is built for Windows file sharing across AZs.

- C: Incorrect. EFS is for Linux, not Windows.

- D: Incorrect. EBS volumes cannot be shared across AZs.

Question: 787

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

Options:
A. Create an Amazon RDS DB instance in Multi-AZ mode.
B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Answer: AD

Explanation:

- A: Correct. RDS Multi-AZ provides HA for the database.

- B: Incorrect. Read replicas don't provide full HA.

- C: Incorrect. EC2-based Docker cluster adds ops burden.

- D: Correct. ECS Fargate is serverless, scales automatically.

- E: Incorrect. EC2 launch type adds more management.

Question: 788

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

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

Answer: A

Explanation:

- A: Correct. AWS Transfer Family provides managed SFTP with direct S3 integration.

- B: Incorrect. S3 File Gateway is for on-premises, not for SFTP endpoints.

- C: Incorrect. EC2 + VPN adds heavy ops burden.

- D: Incorrect. Custom EC2 SFTP cluster requires management.

Question: 789

A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)

Options:

A. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.

B. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.

C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.

D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation.

E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.

Answer: BD

Explanation:

- A: Incorrect. Governance mode can be bypassed by privileged users.

- B: Correct. Compliance mode enforces WORM retention.

- C: Incorrect. SSE-S3 does not support annual key rotation.

- D: Correct. KMS customer managed keys can auto-rotate annually.

- E: Incorrect. Customer-provided keys require manual rotation.

Question: 790

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

Which solution will meet these requirements?

Options:

A. Create an Amazon S3 bucket. Enable static web hosting on the S3 bucket. Upload the static content to the S3 bucket. Use AWS Lambda to process all dynamic content.

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

C. Deploy the web application to Amazon EC2 instances that are configured with Java and PHP. Use Auto Scaling groups and an Application Load Balancer to manage the website's availability.

D. Containerize the web application. Deploy the web application to Amazon EC2 instances. Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.

Answer: B

Explanation:

- A: Incorrect. S3 + Lambda doesn't fit Java/PHP dynamic app fully.

- B: Correct. Elastic Beanstalk provides managed scaling and easy URL swapping for testing.

- C: Incorrect. EC2-based adds ops overhead.

Question: 791

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

Options:
A. Create a read replica. Move reporting queries to the read replica.
B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.
D. Schedule the reporting queries for non-peak hours.

Answer: A

Explanation:

- A: Correct. Read replicas offload reporting traffic from the main DB.

- B: Incorrect. Application should only write to primary, not both.

- C: Incorrect. Migration to DynamoDB is unnecessary.

- D: Incorrect. Doesn't eliminate timeouts, only delays reporting.

Question: 792

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

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

Answer: BE

Explanation:

- A: Incorrect. EC2 + MySQL is not scalable.

- B: Correct. S3 + Athena allows SQL queries at scale.

- C: Incorrect. Custom EC2 adds operational overhead.

- D: Incorrect. Rekognition + Transcribe Medical is not for scanned text.

- E: Correct. Textract + Comprehend Medical extracts medical data efficiently.

Question: 793

A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of reads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.

What should the solutions architect do to meet this requirement?

Options:

A. Add Amazon RDS read replicas.
B. Use Amazon ElastiCache for Redis.
C. Use Amazon Route 53 DNS caching.
D. Use Amazon ElastiCache for Memcached.

Answer: A

Explanation:

- A: Correct. RDS read replicas reduce read load and provide HA.

- B: Incorrect. Redis cache helps but requires app changes.

- C: Incorrect. Route 53 DNS caching is unrelated.

- D: Incorrect. Memcached also requires app logic.

Question: 794

A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application's database. The database must be highly available and must fail over automatically if a disruptive event occurs.

Which solution will meet these requirements?

Options:

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

Answer: A

Explanation:

- A: Correct. Multi-AZ cluster with replication ensures HA and failover.

- B: Incorrect. CloudFormation redeploy is not automatic failover.

- C: Incorrect. Cross-Region is more DR, not HA.

- D: Incorrect. Automatic recovery only restores same instance, not HA.

Question: 795

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

Options:

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

Answer: C

Explanation:

- A: Incorrect. EventBridge doesn't guarantee message persistence.

- B: Incorrect. ALB won't buffer failed requests.

- C: Correct. SQS decouples requests, ensures no loss during outages.

- D: Incorrect. SNS doesn't guarantee durable processing for EC2.

Question: 796

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.
Which solution meets these requirements?

Options:

A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Answer: D

Explanation:

- A: Incorrect. Redeploying stacks is inefficient.

- B: Incorrect. EC2-based monitoring adds unnecessary cost.

- C: Incorrect. Custom Lambda cleanup adds operational overhead.

- D: Correct. DynamoDB TTL automatically deletes old items.

Question: 797
A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.
Which combination of actions should the company take to meet these requirements? (Choose two.)

Options:
A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Answer: BE

Explanation:

- A: Incorrect. Refactoring into serverless requires major development changes, not aligned with the requirement.

- B: Correct. Elastic Beanstalk with .NET in Multi-AZ reduces ops overhead and provides HA with minimal code change.

- C: Incorrect. Using Linux AMI won't support .NET Windows workload natively.

- D: Incorrect. DynamoDB would require code changes since the app currently uses Oracle.

- E: Correct. Oracle on RDS Multi-AZ provides HA while keeping database engine compatibility.

Question: 798

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage. The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.

Which solution meets these requirements?

Options:

A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.

B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage.

C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.

D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Answer: D

Explanation:

- A: Incorrect. MongoDB on EC2 increases ops overhead (patching, scaling, HA).

- B: Incorrect. DynamoDB is not MongoDB-compatible, would need app code changes.

- C: Incorrect. Same issue — DynamoDB isn't MongoDB-compatible.

- D: Correct. EKS with Fargate eliminates cluster management; DocumentDB provides MongoDB compatibility with minimal code change.

Question: 799

A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple speaker recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing purposes.

Which solution will meet these requirements?

Options:

A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.

B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.

C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.

D. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.

Answer: B

Explanation:

- A: Incorrect. Rekognition is for image/video recognition, not audio transcription.

- B: Correct. Transcribe supports speaker identification; Athena can query transcripts in S3.

- C: Incorrect. Translate is for language translation, not speaker recognition.

- D: Incorrect. Textract extracts text from documents, not audio.

Question: 800

A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Configure an AWS Lambda function to be an authorizer in API Gateway to validate which user made the request.

B. For each user, create and assign an API key that must be sent with each request. Validate the key by using an AWS Lambda function.

C. Send the user's email address in the header with every request. Invoke an AWS Lambda function to validate that the user with that email address has proper access.

D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.

Answer: D

Explanation:

- A: Incorrect. Lambda authorizer adds extra ops overhead compared to managed integration.

- B: Incorrect. Creating API keys per user is unscalable and requires extra Lambda code.

- C: Incorrect. Passing email headers and manual validation is insecure and inefficient.

- D: Correct. Cognito user pool authorizer integrates directly with API Gateway, fully managed and minimal effort.

Question: 801

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

A. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.

B. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.

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

D. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.

Answer: C

Question: 802

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Choose two.)

A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance

B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.

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

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

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

Answer: CE

Question: 803

A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.

What should the company do to obtain access to customer accounts in the MOST secure way?

A. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.

B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.

C. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.

D. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Answer: A

Question: 804

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

What is the MOST operationally efficient solution to connect the VPCs?

A. Set up VPC peering connections between each VPC. Update each associated subnet's route table

B. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet

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

D. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team's AWS account to connect to each VPC.

Answer: C

Question: 805

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

Which solution will provide EC2 instances to meet these requirements MOST cost-effectively?

A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.

B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses.

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

D. Create a new launch template for the Auto Scaling group. Increase the instance size. Set a policy to scale out based on CPU usage.

Answer: C

Question: 806

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

A. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.

B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.

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

D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

Answer: C

Question: 807
A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.
The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent.
Which solution should a solutions architect recommend to meet these requirements?

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

Answer: A

Question: 808
A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2 instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.
In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.
Which solutions will meet these requirements with the LEAST administrative effort? (Choose two.)

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

Answer: BD

Question 809:
A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets. Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution. What should the solutions architect recommend to meet this requirement?

Options:
A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Answer: B

Explanation:

- Option B is correct because NACLs support deny rules and can block malicious IPs at subnet level immediately.

- Option A is wrong because security groups cannot have explicit deny rules.

- Option C is wrong because the attack is on the web tier, not the application tier.

- Option D is wrong because blocking at the application tier does not solve the problem upstream.

Question 810:
A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2. Which network design will meet these requirements?

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

Answer: C

Explanation:

- Option C is correct because VPC peering plus updated routes and SG rules enables secure cross-Region communication.

- Option A is wrong because SGs cannot directly reference across Regions.

- Option B is wrong because cross-Region SG referencing is unsupported.

- Option D is wrong because transit gateway peering is unnecessary overhead for just two VPCs.

Question 811:
A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's developers. On average, each development environment is used for half of the 8-hour workday. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Configure each development environment with its own Amazon Aurora PostgreSQL database
B. Configure each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instances
C. Configure each development environment with its own Amazon Aurora On-Demand PostgreSQL-Compatible database
D. Configure each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select

Answer: C

Explanation:

- Option C is correct because Aurora On-Demand (Serverless v2) scales automatically and only charges for usage, reducing cost.

- Option A is wrong because provisioned Aurora instances incur cost even when idle.

- Option B is wrong because RDS Single-AZ instances also charge continuously, regardless of usage.

- Option D is wrong because S3 is object storage, not a relational database.

Question 812:
A company uses AWS Organizations with resources tagged by account. The company also uses AWS Backup to back up its AWS infrastructure resources. The company needs to back up all AWS resources. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use AWS Config to identify all untagged resources. Tag the identified resources programmatically. Use tags in the backup plan.
B. Use AWS Config to identify all resources that are not running. Add those resources to the backup vault.
C. Require all AWS account owners to review their resources to identify the resources that need to be backed up.
D. Use Amazon Inspector to identify all noncompliant resources.

Answer: A

Explanation:

- Option A is correct because tagging ensures complete resource coverage and integrates easily with AWS Backup plans.

- Option B is wrong because backup is needed for running and non-running resources, not just stopped ones.

- Option C is wrong because manual review adds overhead and inconsistency.

- Option D is wrong because Inspector is for security assessment, not backup.

Question 813:
A social media company wants to allow its users to upload images in an application that is hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability. What should a solutions architect do to meet these requirements?

Options:
A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.
B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the images and store the images in an Amazon RDS database.
C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance. Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.
D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs.

Answer: A

Explanation:

- Option A is correct because S3 + Lambda provides a serverless, scalable, event-driven resizing solution.

- Option B is wrong because RDS is not for image storage, and Step Functions add unnecessary complexity.

- Option C is wrong because EC2 adds operational overhead and is less scalable.

- Option D is wrong because ECS/EC2 resizing is more complex than required.

Question 814:

A company is running a microservices application on Amazon EC2 instances. The company wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance. The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster. Which solution will allow the node to join the cluster?

Options:

A. Grant the required permission in AWS Identity and Access Management (IAM) to the AmazonEKSNodeRole IAM role.
B. Create interface VPC endpoints to allow nodes to access the control plane.
C. Recreate nodes in the public subnet. Restrict security groups for EC2 nodes.
D. Allow outbound traffic in the security group of the nodes.

Answer: B

Explanation:

- Option B is correct because with private-only control plane, nodes need interface VPC endpoints to communicate.

- Option A is wrong because IAM roles do not solve networking issues.

- Option C is wrong because moving nodes to public subnets violates compliance.

- Option D is wrong because security group outbound traffic is not enough without private endpoints.

Question 815:

A company is migrating an on-premises application to AWS. The company wants to use Amazon Redshift as a solution. Which use cases are suitable for Amazon Redshift in this scenario? (Choose three.)

Options:

A. Supporting data APIs to access data with traditional, containerized, and event-driven applications
B. Supporting client-side and server-side encryption
C. Building analytics workloads during specified hours and when the application is not active
D. Caching data to reduce the pressure on the backend database
E. Scaling globally to support petabytes of data and tens of millions of requests per minute
F. Creating a secondary replica of the cluster by using the AWS Management Console

Answer: B, C, E

Explanation:

- Option B is correct because Redshift supports encryption for secure data.

- Option C is correct because Redshift is ideal for analytics workloads.

- Option E is correct because Redshift scales to petabytes for analytics queries.

- Option A is wrong because APIs for transactional access are not Redshift's use case.

- Option D is wrong because caching is handled by ElastiCache, not Redshift.

- Option F is wrong because secondary replicas are not created via console like RDS; Redshift uses clusters.

Question 816:
A company provides an API interface to customers so the customers can retrieve their financial information. The company expects a larger number of requests during peak usage times of the year. The company requires the API to respond consistently with low latency to ensure customer satisfaction. The company needs to provide a compute host for the API. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use an Application Load Balancer and Amazon Elastic Container Service (Amazon ECS).
B. Use Amazon API Gateway and AWS Lambda functions with provisioned concurrency.
C. Use an Application Load Balancer and an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.
D. Use Amazon API Gateway and AWS Lambda functions with reserved concurrency.

Answer: B

Explanation:

- Option B is correct because API Gateway + Lambda with provisioned concurrency ensures consistent low latency and low ops.

- Option A is wrong because ECS requires container management overhead.

- Option C is wrong because EKS has higher operational burden.

- Option D is wrong because reserved concurrency doesn't guarantee warm start performance.

Question 817:
A company wants to send all AWS Systems Manager Session Manager logs to an Amazon S3 bucket for archival purposes. Which solution will meet this requirement with the MOST operational efficiency?

Options:
A. Enable S3 logging in the Systems Manager console. Choose an S3 bucket to send the session data to.
B. Install the Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Export the logs to an S3 bucket from the group for archival purposes.
C. Create a Systems Manager document to upload all server logs to a central S3 bucket. Use Amazon EventBridge to run the Systems Manager document against all servers that are in the account daily.
D. Install an Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Create a CloudWatch logs subscription that pushes any incoming log events to an Amazon Kinesis Data Firehose delivery stream. Set Amazon S3 as the destination.

Answer: A

Explanation:

- Option A is correct because Session Manager has built-in integration with S3, requiring minimal setup.

- Option B is wrong because CloudWatch export adds extra steps.

- Option C is wrong because custom documents add unnecessary overhead.

- Option D is wrong because Firehose + CloudWatch integration adds complexity.

Question 818:
An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

Options:
A. Enable storage autoscaling in RDS
B. Increase the RDS database instance size
C. Change the RDS database instance storage type to Provisioned IOPS
D. Back up the RDS database, increase the storage capacity, restore the database, and stop the previous instance

Answer: A

Explanation:

- Option A is correct because RDS storage autoscaling automatically grows storage without downtime.

- Option B is wrong because increasing instance size doesn't increase storage capacity.

- Option C is wrong because changing storage type doesn't address capacity.

- Option D is wrong because backup/restore causes downtime.

Question 819:
A consulting company provides professional services to customers worldwide. The company provides solutions and tools for customers to expedite gathering and analyzing data on AWS. The company needs to centrally manage and deploy a common set of solutions and tools for customers to use for self-service purposes. Which solution will meet these requirements?

Options:
A. Create AWS CloudFormation templates for the customers.
B. Create AWS Service Catalog products for the customers.
C. Create AWS Systems Manager templates for the customers.
D. Create AWS Config items for the customers.

Answer: B

Explanation:

- Option B is correct because AWS Service Catalog allows centralized management of products for self-service.

- Option A is wrong because CloudFormation alone lacks centralized product governance.

- Option C is wrong because Systems Manager templates are for automation, not cataloging.

- Option D is wrong because AWS Config is for compliance, not self-service deployment.

Question 820:
A company is designing a new web application that will run on Amazon EC2 Instances. The application will use Amazon DynamoDB for backend data storage. The application traffic will be unpredictable. The company expects that the application read and write throughput to the database will be moderate to high. The company needs to scale in response to application traffic. Which DynamoDB table configuration will meet these requirements MOST cost-effectively?

Options:
A. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard table class. Set DynamoDB auto scaling to a maximum defined capacity.
B. Configure DynamoDB in on-demand mode by using the DynamoDB Standard table class.
C. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.
D. Configure DynamoDB in on-demand mode by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class.

Answer: B

Explanation:

- Option B is correct because on-demand mode scales automatically and is cost-effective for unpredictable traffic.

- Option A is wrong because provisioned mode risks over/under-provisioning.

- Option C is wrong because Standard-IA is for archival data, not active workloads.

- Option D is wrong because Standard-IA with on-demand is not intended for frequent access.

Question 821:
A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account. The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables. Which authentication option will meet these requirements MOST securely?

Options:
A. Integrate DynamoDB with AWS Secrets Manager in the inventory application account. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB table. Schedule secret rotation for every 30 days.
B. In every business account, create an IAM user that has programmatic access. Configure the application to use the correct IAM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate IAM access keys every 30 days.
C. In every business account, create an IAM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application account. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operation. Configure the application to use APP_ROLE and assume the cross-account role BU_ROLE to read the DynamoDB table.
D. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoDB. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Answer: C

Explanation:

- Option C is correct because cross-account IAM roles with AssumeRole provide secure, temporary access.

- Option A is wrong because Secrets Manager is not meant for DynamoDB cross-account access.

- Option B is wrong because IAM users with keys are insecure and require manual rotation.

- Option D is wrong because ACM certificates don't provide authentication for DynamoDB.

Question 822:
A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS). The company's workload is not consistent throughout the day. The company wants Amazon EKS to scale in and out according to the workload. Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

Options:
A. Use an AWS Lambda function to resize the EKS cluster.
B. Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.
C. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.
D. Use Amazon API Gateway and connect it to Amazon EKS.
E. Use AWS App Mesh to observe network activity.

Answer: B, C

Explanation:

- Option B is correct because Metrics Server enables horizontal pod autoscaling.

- Option C is correct because Cluster Autoscaler manages node scaling automatically.

- Option A is wrong because resizing clusters with Lambda is manual and inefficient.

- Option D is wrong because API Gateway does not handle scaling for EKS.

- Option E is wrong because App Mesh is for observability, not scaling.

Question 823:
A company runs a microservice-based serverless web application. The application must be able to retrieve data from multiple Amazon DynamoDB tables. A solutions architect needs to give the application the ability to retrieve the data with no impact on the baseline performance of the application. Which solution will meet these requirements in the MOST operationally efficient way?

Options:
A. AWS AppSync pipeline resolvers
B. Amazon CloudFront with functions
C. Edge-optimized Amazon API Gateway with AWS Lambda functions
D. Amazon Athena Federated Query with a DynamoDB connector

Answer: A

Explanation:

- Option A is correct because AppSync can aggregate queries across multiple DynamoDB tables efficiently.

- Option B is wrong because CloudFront + Lambda@Edge is for content delivery, not querying databases.

- Option C is wrong because API Gateway + Lambda increases latency and overhead.

- Option D is wrong because Athena Federated Query is for ad-hoc analytics, not low-latency application queries.

Question 824:
A company wants to analyze and troubleshoot Access Denied errors and Unauthorized errors that are related to IAM permissions. The company has AWS CloudTrail turned on. Which solution will meet these requirements with the LEAST effort?

Options:
A. Use AWS Glue and write custom scripts to query CloudTrail logs for the errors.
B. Use AWS Batch and write custom scripts to query CloudTrail logs for the errors.
C. Search CloudTrail logs with Amazon Athena queries to identify the errors.
D. Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.

Answer: C

Explanation:

- Option C is correct because Athena can directly query CloudTrail logs stored in S3 with minimal setup.

- Option A is wrong because Glue scripts add complexity.

- Option B is wrong because Batch is unnecessary for simple queries.

- Option D is wrong because QuickSight is visualization, not query analysis.

Question 825:
A company wants to add its existing AWS usage cost to its operation cost dashboard. A solutions architect needs to recommend a solution that will give the company access to its usage cost programmatically. The company must be able to access cost data for the current year and forecast costs for the next 12 months. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Access usage cost-related data by using the AWS Cost Explorer API with pagination.
B. Access usage cost-related data by using downloadable AWS Cost Explorer report .csv files.
C. Configure AWS Budgets actions to send usage cost data to the company through FTP.
D. Create AWS Budgets reports for usage cost data. Send the data to the company through SMTP.

Answer: A

Explanation:

- Option A is correct because the Cost Explorer API provides programmatic access with forecasting.

- Option B is wrong because downloading CSVs is manual and less efficient.

- Option C is wrong because Budgets actions don't provide full forecasting data via FTP.

- Option D is wrong because Budgets reports sent via SMTP are not programmatic access.

Question 826:
A solutions architect is reviewing the resilience of an application. The solutions architect notices that a database administrator recently failed over the application's Amazon Aurora PostgreSQL database writer instance as part of a scaling exercise. The failover resulted in 3 minutes of downtime for the application. Which solution will reduce the downtime for scaling exercises with the LEAST operational overhead?

Options:
A. Create more Aurora PostgreSQL read replicas in the cluster to handle the load during failover.
B. Set up a secondary Aurora PostgreSQL cluster in the same AWS Region. During failover, update the application to use the secondary cluster's writer endpoint.
C. Create an Amazon ElastiCache for Memcached cluster to handle the load during failover.
D. Set up an Amazon RDS Proxy for the database. Update the application to use the proxy endpoint.

Answer: D

Explanation:

- Option D is correct because RDS Proxy reduces failover time by managing connections.

- Option A is wrong because read replicas don't reduce writer failover downtime.

- Option B is wrong because switching to another cluster requires app changes.

- Option C is wrong because caching does not solve failover delays.

Question 827:
A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora global database cluster that extends across multiple Availability Zones. The company wants to expand globally and to ensure that its application has minimal downtime. Which solution will provide the MOST fault tolerance?

Options:
A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL cross-Region Aurora Replica in the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.
C. Deploy the web tier and the application tier to a second Region. Create an Aurora PostgreSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

Answer: D

Explanation:

- Option D is correct because Aurora global database provides cross-Region disaster recovery with minimal downtime.

- Option A is wrong because extending Auto Scaling across Regions doesn't cover failover properly.

- Option B is wrong because cross-Region replicas require manual promotion.

- Option C is wrong because DMS replication introduces latency and downtime risk.

Question 828:

A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. An on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running. The company wants the AWS solution to process incoming data files as soon as possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files after the files have been processed successfully. Processing for each file needs to take 3–8 minutes. Which solution will meet these requirements in the MOST operationally efficient way?

Options:

A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.

B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files nightly from the EBS volume. Delete the files after the job has processed the files.

C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each file arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.

D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Answer: D

Explanation:

- Option D is correct because Transfer Family with S3 integrates easily and triggers Lambda for near-real-time processing.

- Option A is wrong because Glacier is for archival storage, not active processing.

- Option B is wrong because EBS + nightly processing delays data handling.

- Option C is wrong because EBS doesn't integrate as seamlessly as S3 for event-driven workflows.

Question 829:

A company is migrating its workloads to AWS. The company has transactional and sensitive data in its databases. The company wants to use AWS Cloud solutions to increase security and reduce operational overhead for the databases. Which solution will meet these requirements?

Options:

A. Migrate the databases to Amazon EC2. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.

B. Migrate the databases to Amazon RDS. Configure encryption at rest.

C. Migrate the data to Amazon S3. Use Amazon Macie for data security and protection.

D. Migrate the database to Amazon RDS. Use Amazon CloudWatch Logs for data security and protection.

Answer: B

Explanation:

- Option B is correct because RDS provides managed databases with encryption at rest, reducing ops overhead.

- Option A is wrong because managing databases on EC2 increases overhead.

- Option C is wrong because transactional data is not suitable for S3.

- Option D is wrong because CloudWatch Logs is for monitoring, not database security.

Question 830:

A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth. Which solution will meet these requirements?

Options:

A. Add an Amazon CloudFront distribution in front of the NLBs. Increase the Cache-Control max-age parameter.

B. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.

C. Add AWS Global Accelerator in front of the NLBs. Configure a Global Accelerator endpoint to use the correct listener ports.

D. Add an Amazon API Gateway endpoint behind the NLBs. Enable API caching. Override method caching for the different stages.

Answer: C

Explanation:

- Option C is correct because Global Accelerator provides static IPs, reduces latency, and optimizes routing globally.

- Option A is wrong because CloudFront is for HTTP/HTTPS, not TCP/UDP gaming.

- Option B is wrong because ALBs don't support UDP.

- Option D is wrong because API Gateway is not designed for gaming protocols.

Question 831:
A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption. A developer wrote an AWS Lambda function to retrieve data when the company receives a webhook callback. The developer must make the Lambda function available for the third party to call. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A. Create a function URL for the Lambda function. Provide the Lambda function URL to the third party for the webhook.
B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook.
C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook.
D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lambda function. Provide the public hostname of the SQS queue to the third party for the webhook.

Answer: A

Explanation:

- Option A is correct because Lambda function URLs provide direct HTTPS endpoints with minimal configuration.

- Option B is wrong because ALB adds unnecessary infrastructure overhead.

- Option C is wrong because SNS endpoints are not webhook-compatible for direct third-party callbacks.

- Option D is wrong because SQS is a queue, not a webhook endpoint.

Question 832:
A company has a workload in an AWS Region. Customers connect to and access the workload by using an Amazon API Gateway REST API. The company uses Amazon Route 53 as its DNS provider. The company wants to provide individual and secure URLs for all customers. Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three.)

Options:
A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint.
B. Request a wildcard certificate that matches the domains in AWS Certificate Manager (ACM) in a different Region.
C. Create hosted zones for each customer as required in Route 53. Create zone records that point to the API Gateway endpoint.
D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.
E. Create multiple API endpoints for each customer in API Gateway.
F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM).

Answer: A, D, F

Explanation:

- Option A is correct because wildcard domains simplify per-customer URLs.

- Option D is correct because certificates must match the wildcard domain in the same Region.

- Option F is correct because custom domains in API Gateway provide secure endpoints.

- Option B is wrong because the certificate must be in the same Region, not a different one.

- Option C is wrong because hosted zones for each customer add too much overhead.

- Option E is wrong because multiple API endpoints duplicate work unnecessarily.

Question 833:
A company stores data in Amazon S3. According to regulations, the data must not contain personally identifiable information (PII). The company recently discovered that S3 buckets have some objects that contain PII. The company needs to automatically detect PII in S3 buckets and to notify the company's security team. Which solution will meet these requirements?

Options:
A. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData event type from Macie findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
B. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
C. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData:S3Object/Personal event type from Macie findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.
D. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

Answer: A

Explanation:

- Option A is correct because Macie is purpose-built for detecting PII and integrates with EventBridge + SNS.

- Option B is wrong because GuardDuty is for threat detection, not PII.

- Option C is wrong because SNS is better suited for notifications than SQS here.

- Option D is wrong because GuardDuty is unrelated to data classification.

Question 834:
A company wants to build a logging solution for its multiple AWS accounts. The company currently stores the logs from all accounts in a centralized account. The company has created an Amazon S3 bucket in the centralized account to store the VPC flow logs and AWS CloudTrail logs. All logs must be highly available for 30 days for frequent analysis, retained for an additional 60 days for backup purposes, and deleted 90 days after creation. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Transition objects to the S3 Standard storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
B. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
C. Transition objects to the S3 Glacier Flexible Retrieval storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
D. Transition objects to the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.

Answer: C

Explanation:

- Option C is correct because Glacier provides low-cost storage for backup retention, and lifecycle rules manage expiration.

- Option A is wrong because S3 Standard is costly for backup storage.

- Option B is wrong because objects are deleted at 90 days, not moved again.

- Option D is wrong because One Zone-IA is less durable and unnecessary here.

Question 835:
A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store. Which solution will meet these requirements?

Options:
A. Create a new AWS Key Management Service (AWS KMS) key. Use AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS.
B. Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.
C. Create the Amazon EKS cluster with default options. Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.
D. Create a new AWS Key Management Service (AWS KMS) key with the alias/aws/ebs alias. Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Answer: B

Explanation:

- Option B is correct because enabling KMS secrets encryption secures etcd key-value store in EKS.

- Option A is wrong because Secrets Manager is external, not for etcd encryption.

- Option C is wrong because EBS CSI driver manages volumes, not secrets.

- Option D is wrong because EBS encryption doesn't apply to Kubernetes secrets.

Question 836:
A company wants to provide data scientists with near real-time read-only access to the company's production Amazon RDS for PostgreSQL database. The database is currently configured as a Single-AZ database. The data scientists use complex queries that will not affect the production database. The company needs a solution that is highly available. Which solution will meet these requirements MOST cost-effectively?

Options:
A. Scale the existing production database in a maintenance window to provide enough power for the data scientists.
B. Change the setup from a Single-AZ to a Multi-AZ instance deployment with a larger secondary standby instance. Provide the data scientists access to the secondary instance.
C. Change the setup from a Single-AZ to a Multi-AZ instance deployment. Provide two additional read replicas for the data scientists.
D. Change the setup from a Single-AZ to a Multi-AZ cluster deployment with two readable standby instances. Provide read endpoints to the data scientists.

Answer: C

Explanation:

- Option C is correct because read replicas offload queries and ensure availability at lower cost than clusters.

- Option A is wrong because scaling production increases cost and doesn't offload queries.

- Option B is wrong because Multi-AZ standby is not readable.

- Option D is wrong because Multi-AZ clusters are costlier than needed.

Question 837:
A company runs a three-tier web application in the AWS Cloud that operates across three Availability Zones. The application architecture has an Application Load Balancer, an Amazon EC2 web server that hosts user session states, and a MySQL database that runs on an EC2 instance. The company expects sudden increases in application traffic. The company wants to be able to scale to meet future application capacity demands and to ensure high availability across all three Availability Zones. Which solution will meet these requirements?

Options:
A. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
B. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Memcached with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
C. Migrate the MySQL database to Amazon DynamoDB. Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
D. Migrate the MySQL database to Amazon RDS for MySQL in a single Availability Zone. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

Answer: A

Explanation:

- Option A is correct because RDS Multi-AZ + ElastiCache Redis + Auto Scaling gives high availability and scalability.

- Option B is wrong because Redis is better than Memcached for session data.

- Option C is wrong because re-architecting to DynamoDB is unnecessary.

- Option D is wrong because single AZ database reduces resilience.

Question 838:
A global video streaming company uses Amazon CloudFront as a content distribution network (CDN). The company wants to roll out content in a phased manner across multiple countries. The company needs to ensure that viewers who are outside the countries to which the company rolls out content are not able to view the content. Which solution will meet these requirements?

Options:
A. Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
B. Set up a new URL for restricted content. Authorize access by using a signed URL and cookies. Set up a custom error message.
C. Encrypt the data for the content that the company distributes. Set up a custom error message.
D. Create a new URL for restricted content. Set up a time-restricted access policy for signed URLs.

Answer: A

Explanation:

- Option A is correct because CloudFront geographic restrictions enforce country-level allow lists.

- Option B is wrong because signed URLs control user access, not geography.

- Option C is wrong because encryption doesn't block by geography.

- Option D is wrong because time-restricted URLs control duration, not location.

Question 839:
A company wants to use the AWS Cloud to improve its on-premises disaster recovery (DR) configuration. The company's core production business application uses Microsoft SQL Server Standard, which runs on a virtual machine (VM). The application has a recovery point objective (RPO) of 30 seconds or fewer and a recovery time objective (RTO) of 60 minutes. The DR solution needs to minimize costs wherever possible. Which solution will meet these requirements?

Options:
A. Configure a multi-site active/active setup between the on-premises server and AWS by using Microsoft SQL Server Enterprise with Always On availability groups.
B. Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
C. Use AWS Elastic Disaster Recovery configured to replicate disk changes to AWS as a pilot light.
D. Use third-party backup software to capture backups every night. Store a secondary set of backups in Amazon S3.

Answer: B

Explanation:

- Option B is correct because RDS SQL Server with DMS CDC meets RPO and RTO while minimizing costs.

- Option A is wrong because Enterprise Always On licensing is expensive.

- Option C is wrong because Elastic DR pilot light may not meet the 30-second RPO.

- Option D is wrong because nightly backups exceed the RPO requirement.

Question 840:
A company has an on-premises server that uses an Oracle database to process and store customer information. The company wants to use an AWS database service to achieve higher availability and to improve application performance. The company also wants to offload reporting from its primary database system. Which solution will meet these requirements in the MOST operationally efficient way?

Options:
A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance.
B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database. Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica.
C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.
D. Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database. Direct the reporting functions to the reader instances.

Answer: C

Explanation:

- Option C is correct because RDS Multi-AZ cluster deployments with readers offload reporting and ensure high availability.

- Option A is wrong because multi-Region adds unnecessary complexity.

- Option B is wrong because Single-AZ with a replica doesn't ensure high availability.

- Option D is wrong because Aurora is not Oracle-compatible.

Question 841:
A company wants to build a web application on AWS. Client access requests to the website are not predictable and can be idle for a long time. Only customers who have paid a subscription fee can have the ability to sign in and use the web application. Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

Options:
A. Create an AWS Lambda function to retrieve user information from Amazon DynamoDB. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.
B. Create an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to retrieve user information from Amazon RDS. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.

C. Create an Amazon Cognito user pool to authenticate users.
D. Create an Amazon Cognito identity pool to authenticate users.
E. Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated Amazon CloudFront configuration.
F. Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

Answer: A, C, E

Explanation:

- Option A is correct because Lambda + API Gateway is serverless and cost-effective for unpredictable traffic.

- Option C is correct because Cognito provides user authentication.

- Option E is correct because Amplify + CloudFront serves web content efficiently.

- Option B is wrong because ECS + RDS is not cost-effective for unpredictable workloads.

- Option D is wrong because identity pools are not needed here.

- Option F is wrong because S3 with PHP is not supported natively.

Question 842:
A media company uses an Amazon CloudFront distribution to deliver content over the internet. The company wants only premium customers to have access to the media streams and file content. The company stores all content in an Amazon S3 bucket. The company also delivers content on demand to customers for a specific purpose, such as movie rentals or music downloads. Which solution will meet these requirements?

Options:
A. Generate and provide S3 signed cookies to premium customers.
B. Generate and provide CloudFront signed URLs to premium customers.
C. Use origin access control (OAC) to limit the access of non-premium customers.
D. Generate and activate field-level encryption to block non-premium customers.

Answer: B

Explanation:

- Option B is correct because CloudFront signed URLs provide secure access to premium content and rentals.

- Option A is wrong because S3 signed cookies don't integrate directly with CloudFront.

- Option C is wrong because OAC restricts origin access, not user-level access.

- Option D is wrong because field-level encryption is unrelated to premium access control.

Question 843:
A company runs Amazon EC2 instances in multiple AWS accounts that are individually billed. The company recently purchased a Savings Plan. Because of changes in the company's business requirements, the company has decommissioned a large number of EC2 instances. The company wants to use its Savings Plan discounts on its other AWS accounts. Which combination of steps will meet these requirements? (Choose two.)

Options:
A. From the AWS Account Management Console of the management account, turn on discount sharing from the billing preferences section.
B. From the AWS Account Management Console of the account that purchased the existing Savings Plan, turn on discount sharing from the billing preferences section. Include all accounts.
C. From the AWS Organizations management account, use AWS Resource Access Manager (AWS RAM) to share the Savings Plan with other accounts.
D. Create an organization in AWS Organizations in a new payer account. Invite the other AWS accounts to join the organization from the management account.
E. Create an organization in AWS Organizations in the existing AWS account with the existing EC2 instances and Savings Plan. Invite the other AWS accounts to join the organization from the management account.

Answer: A, E

Explanation:

- Option A is correct because discount sharing must be enabled in billing preferences.

- Option E is correct because creating an organization in the existing account consolidates billing.

- Option B is wrong because discount sharing is managed by the organization's management account.

- Option C is wrong because RAM does not share Savings Plans.

- Option D is wrong because creating a new payer account is unnecessary.

Question 844:
A retail company uses a regional Amazon API Gateway API for its public REST APIs. The API Gateway endpoint is a custom domain name that points to an Amazon Route 53 alias record. A solutions architect needs to create a solution that has minimal effects on customers and minimal data loss to release the new version of APIs. Which solution will meet these requirements?

Options:
A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.
B. Create a new API Gateway endpoint with a new version of the API in OpenAPI YAML file format. Use the import-to-update operation in merge mode into the API in API Gateway. Deploy the new version of the API to the production stage.
C. Create a new API Gateway endpoint with a new version of the API in OpenAPI JSON file format. Use the import-to-update operation in overwrite mode into the API in API Gateway. Deploy the new version of the API to the production stage.
D. Create a new API Gateway endpoint with new versions of the API definitions. Create a custom domain name for the new API Gateway API. Point the Route 53 alias record to the new API Gateway API custom domain name.

Answer: A

Explanation:

- Option A is correct because canary deployments in API Gateway allow phased rollout with minimal customer impact.

- Option B is wrong because merge mode overwrites and may cause inconsistency.

- Option C is wrong because overwrite mode risks downtime and data loss.

- Option D is wrong because changing domains causes customer disruption.

Question 845:
A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead. Which solution will meet these requirements?

Options:
A. Update the Route 53 records to use a latency routing policy. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
D. Update the Route 53 records to use a multivalue answer routing policy. Create a health check. Direct traffic to the website if the health check passes. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

Answer: B

Explanation:

- Option B is correct because active-passive failover with S3 static page provides low overhead fallback.

- Option A is wrong because latency routing is not designed for failover.

- Option C is wrong because adding EC2 adds unnecessary cost and ops.

- Option D is wrong because multivalue answer is not suited for static error page failover.

Question 846:
A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows. What should a solutions architect recommend?

Options:
A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Answer: D

Explanation:

- Option D is correct because Storage Gateway VTL integrates with tape-based workflows seamlessly.

- Option A is wrong because NFS file gateway is for file storage, not tape backup.

- Option B is wrong because EFS is a file system, not tape-compatible.

- Option C is wrong because EFS does not support iSCSI.

Question 847:
A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.
B. Use AWS Glue to deliver streaming data to Amazon S3.
C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.
D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Answer: A

Explanation:

- Option A is correct because Kinesis Data Firehose directly streams to S3 with near real-time and low ops.

- Option B is wrong because Glue is for ETL, not streaming.

- Option C is wrong because Lambda cannot handle high-volume streams efficiently.

- Option D is wrong because DMS is for database replication, not IoT streams.

Question 848:
A company has separate AWS accounts for its finance, data analytics, and development departments. Because of costs and security concerns, the company wants to control which services each AWS account can use. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Use AWS Systems Manager templates to control which AWS services each department can use.
B. Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
C. Use AWS CloudFormation to automatically provision only the AWS services that each department can use.
D. Set up a list of products in AWS Service Catalog in the AWS accounts to manage and control the usage of specific AWS services.

Answer: B

Explanation:

- Option B is correct because SCPs at OU level control allowed/denied services with minimal overhead.

- Option A is wrong because Systems Manager templates don't restrict service usage.

- Option C is wrong because CloudFormation doesn't enforce service restrictions.

- Option D is wrong because Service Catalog is more for provisioning, not service restriction.

Question 849:
A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead. What should the solutions architect do to meet these requirements?

Options:
A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Answer: B

Explanation:

- Option B is correct because a NAT gateway securely allows private subnets to reach the internet.

- Option A is wrong because NAT instances require more management.

- Option C is wrong because private subnets should not use internet gateways directly.

- Option D is wrong because virtual private gateways are for VPNs, not internet.

Question 850:
A company is using AWS Key Management Service (AWS KMS) keys to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables. Which steps must the solutions architect take to implement the correct permissions? (Choose two.)

Options:
A. Add AWS KMS permissions in the Lambda resource policy.
B. Add AWS KMS permissions in the Lambda execution role.
C. Add AWS KMS permissions in the Lambda function policy.
D. Allow the Lambda execution role in the AWS KMS key policy.
E. Allow the Lambda resource policy in the AWS KMS key policy.

Answer: B, D

Explanation:

- Option B is correct because the Lambda execution role must have decrypt permission.

- Option D is correct because the KMS key policy must allow the Lambda execution role.

- Option A is wrong because resource policies are not for KMS permissions.

- Option C is wrong because Lambda function policies don't manage KMS access.

- Option E is wrong because Lambda resource policies are not part of KMS key policies.

Question 851:
A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours. Which solution meets these requirements MOST cost-effectively?

Options:
A.Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.
B.Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
C.Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard- Infrequent Access (S3 Standard-IA) and S3 Glacier.
D.Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Answer: A

Explanation:

- S3 Standard for initial frequent access then transitioning to Glacier provides the best cost efficiency with retrieval within 6 hours.

- Option B (S3 Standard-IA) does not meet the long-term archival requirement as Glacier is cheaper for multi-year storage.

- Option C (Intelligent-Tiering) has monitoring overhead and extra charges, making it less cost-effective for predictable access patterns.

- Option D (Glacier Deep Archive) is not suitable because retrieval can take up to 12 hours, exceeding the 6-hour requirement.

Question 852:
A company needs to optimize the cost of its Amazon EC2 instances. The company also needs to change the type and family of its EC2 instances every 2-3 months. What should the company do to meet these requirements?

Options:
A.Purchase Partial Upfront Reserved Instances for a 3-year term.
B.Purchase a No Upfront Compute Savings Plan for a 1-year term.
C.Purchase All Upfront Reserved Instances for a 1-year term.
D.Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

Answer: B

Explanation:

- Compute Savings Plan with 1-year term and no upfront provides flexibility to change instance types/families while saving costs.

- Option A locks the company into specific instances for 3 years, not suitable for frequent changes.

- Option C still locks into a specific instance type, not flexible enough.

- Option D EC2 Instance Savings Plan is restrictive to EC2, while Compute Savings Plan covers EC2, Fargate, and Lambda.

Question 853:
A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (PII). The company stores the PII data in the us-east-1 Region and us-west-2 Region. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Configure Amazon Macie in each Region. Create a job to analyze the data that is in Amazon S3.
B.Configure AWS Security Hub for all Regions. Create an AWS Config rule to analyze the data that is in Amazon S3.
C.Configure Amazon Inspector to analyze the data that is in Amazon S3.
D.Configure Amazon GuardDuty to analyze the data that is in Amazon S3.

Answer: A

Explanation:

- Amazon Macie is designed for discovering and classifying sensitive data like PII in S3 with minimal setup.

- Option B Security Hub aggregates findings but cannot analyze S3 data directly.

- Option C Inspector is for vulnerabilities in compute resources, not S3.

- Option D GuardDuty detects threats and anomalies, not sensitive data in S3.

Question 854:
Accounts under the same organization in AWS Organizations across multiple AWS Regions. Teams for each product line have tagged each compute resource in the individual accounts. The company wants more details about the cost for each product line from the consolidated billing feature in Organizations. Which combination of steps will meet these requirements? (Choose two.)

Options:
A.Select a specific AWS generated tag in the AWS Billing console.
B.Select a specific user-defined tag in the AWS Billing console.
C.Select a specific user-defined tag in the AWS Resource Groups console.
D.Activate the selected tag from each AWS account.
E.Activate the selected tag from the Organizations management account.

Answer: B, E

Explanation:

- User-defined tags must be activated in the management account and selected in the Billing console for consolidated cost allocation.

- Option A AWS generated tags are limited and not customizable for product lines.

- Option C Resource Groups console is for grouping resources, not billing.

- Option D Activating in each account is not required; activation must be done at the management account level.

Question 855:
A company's solutions architect is designing an AWS multi-account solution that uses AWS Organizations. The solutions architect has organized the company's accounts into organizational units (OUs). The solutions architect needs a solution that will identify any changes to the OU hierarchy. The solution also needs to notify the company's operations team of any changes. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Provision the AWS accounts by using AWS Control Tower. Use account drift notifications to identify the changes to the OU hierarchy.
B.Provision the AWS accounts by using AWS Control Tower. Use AWS Config aggregated rules to identify the changes to the OU hierarchy.
C.Use AWS Service Catalog to create accounts in Organizations. Use an AWS CloudTrail organization trail to identify the changes to the OU hierarchy.
D.Use AWS CloudFormation templates to create accounts in Organizations. Use the drift detection operation on a stack to identify the changes to the OU hierarchy.

Answer: A

Explanation:

- Control Tower provides account drift detection and notifications with minimal effort.

- Option B Config rules require custom setup, increasing operational overhead.

- Option C CloudTrail requires manual tracking and alerting logic

- Option D CloudFormation drift detection is not designed for OU hierarchy changes.

Question 856:
A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the Amazon DynamoDB table. Which solution will meet these requirements with the LEAST amount of operational overhead?

Options:
A.Set up a DynamoDB Accelerator (DAX) cluster. Route all read requests through DAX.
B.Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application. Route all read requests through Redis.
C.Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application. Route all read requests through Memcached.
D.Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Answer: A

Explanation:

- DynamoDB Accelerator (DAX) is a fully managed, purpose-built cache for DynamoDB that reduces latency to microseconds with minimal overhead.

- Option B Redis would work but requires managing cache logic and synchronization.

- Option C Memcached same issue, more management overhead.

- Option D Lambda + Streams introduces unnecessary complexity compared to DAX.

Question 857:
A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet. Which combination of steps should the solutions architect take to meet this requirement? (Choose two.)

Options:
A.Create a route table entry for the endpoint.
B.Create a gateway endpoint for DynamoDB.
C.Create an interface endpoint for Amazon EC2.
D.Create an elastic network interface for the endpoint in each of the subnets of the VPC.
E.Create a security group entry in the endpoint's security group to provide access.

Answer: A, B

Explanation:

- Gateway endpoints for DynamoDB allow traffic to stay within AWS without traversing the internet, and route table entries ensure traffic routing.

- Option C is unnecessary; interface endpoints are not required for DynamoDB.

- Option D is not required; gateway endpoints don't need ENIs.

- Option E not needed because gateway endpoints don't use security groups

Question 858:
A company runs its applications on both Amazon Elastic Kubernetes Service (Amazon EKS) clusters and on-premises Kubernetes clusters. The company wants to view all clusters and workloads from a central location. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use Amazon CloudWatch Container Insights to collect and group the cluster information.
B.Use Amazon EKS Connector to register and connect all Kubernetes clusters.
C.Use AWS Systems Manager to collect and view the cluster information.
D.Use Amazon EKS Anywhere as the primary cluster to view the other clusters with native Kubernetes commands.

Answer: B

Explanation:

- EKS Connector allows central visibility of on-prem and EKS clusters in one console.

- Option A CloudWatch gives metrics/logs but not cluster-level central visibility.

- Option C Systems Manager doesn't manage Kubernetes workloads directly.

- Option D EKS Anywhere is for on-prem Kubernetes deployment, not for visibility.

Question 859:
A company is building an ecommerce application and needs to store sensitive customer information. The company needs to give customers the ability to complete purchase transactions on the website. The company also needs to ensure that sensitive customer data is protected, even from database administrators. Which solution meets these requirements?

Options:
A.Store sensitive data in an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS encryption to encrypt the data. Use an IAM instance role to restrict access.
B.Store sensitive data in Amazon RDS for MySQL. Use AWS Key Management Service (AWS KMS) client-side encryption to encrypt the data.
C.Store sensitive data in Amazon S3. Use AWS Key Management Service (AWS KMS) server-side encryption to encrypt the data. Use S3 bucket policies to restrict access.
D.Store sensitive data in Amazon FSx for Windows Server. Mount the file share on application servers. Use Windows file permissions to restrict access.

Answer: B

Explanation:

- RDS with KMS client-side encryption ensures data is encrypted before reaching DB, protecting even from DBAs.

- Option A EBS encryption protects at storage but DBAs with instance access can see data.

- Option C S3 is not suitable for transactional application data.

- Option D FSx is not meant for secure relational transactional workloads.

Question 860:
A company has an on-premises MySQL database that handles transactional data. The company is migrating the database to the AWS Cloud. The migrated database must maintain compatibility with the company's applications that use the database. The migrated database also must scale automatically during periods of increased demand. Which migration solution will meet these requirements?

Options:
A.Use native MySQL tools to migrate the database to Amazon RDS for MySQL. Configure elastic storage scaling.
B.Migrate the database to Amazon Redshift by using the mysqldump utility. Turn on Auto Scaling for the Amazon Redshift cluster.
C.Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon Aurora. Turn on Aurora Auto Scaling.
D.Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon DynamoDB. Configure an Auto Scaling policy.

Answer: C

Explanation:

- Aurora MySQL compatible supports transactional workloads and auto scaling, ideal for migration.

- Option A RDS MySQL supports auto storage scaling but not compute scaling.

- Option B Redshift is for analytics, not transactional.

- Option D DynamoDB is NoSQL, not compatible with MySQL transactional applications.

Question 861:
A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage. What should a solutions architect do to meet these requirements?

Options:
A.Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.
B.Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each EC2 instance.
C.Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.
D.Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Answer: B

Explanation:

- EFS provides shared, concurrent, scalable file storage across multiple AZs.

- Option A S3 is object storage, not for concurrent hierarchical file system access.

- Option C EBS cannot be attached to multiple instances across AZs.

- Option D syncing EBS across instances adds high complexity and overhead.

Question 862:

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions architect adds independent components. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A.Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.

B.Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.

C.Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.

D.Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.

Answer: A

Explanation:

- API Gateway + Lambda + DynamoDB is fully managed, serverless, and scalable with least ops.

- Option B EC2 and ELB adds infrastructure management.

- Option C SQL Server on EC2 requires high admin effort

- Option D ELB + EFS + EC2 increases operational complexity.

Question 863:

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure. The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

Options:

A.Amazon S3 with Amazon CloudFront

B.Amazon S3 Glacier with Amazon ElastiCache

C.Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront

D.AWS Storage Gateway with Amazon ElastiCache

Answer: A

Explanation:

- S3 for scalable storage + CloudFront for caching provides low latency at scale.

- Option B Glacier is archival, not for frequent access.

- Option C EBS cannot scale to petabytes easily, not cost-efficient.

- Option D Storage Gateway is for hybrid, not required here.

Question 864:
An Amazon EventBridge rule targets a third-party API. The third-party API has not received any incoming traffic. A solutions architect needs to determine whether the rule conditions are being met and if the rule's target is being invoked. Which solution will meet these requirements?

Options:
A.Check for metrics in Amazon CloudWatch in the namespace for AWS/Events.
B.Review events in the Amazon Simple Queue Service (Amazon SQS) dead-letter queue.
C.Check for the events in Amazon CloudWatch Logs.
D.Check the trails in AWS CloudTrail for the EventBridge events.

Answer: A

Explanation:

- CloudWatch metrics for EventBridge show matched events and invocations.

- Option B SQS DLQ only relevant if target is SQS with DLQ configured.

- Option C Logs not enabled by default for EventBridge.

- Option D CloudTrail records API calls, not event matches/invocations.

Question 865:
A company has a large workload that runs every Friday evening. The workload runs on Amazon EC2 instances that are in two Availability Zones in the us-east-1 Region. Normally, the company must run no more than two instances at all times. However, the company wants to scale up to six instances each Friday to handle a regularly repeating increased workload. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Create a reminder in Amazon EventBridge to scale the instances.
B.Create an Auto Scaling group that has a scheduled action.
C.Create an Auto Scaling group that uses manual scaling.
D.Create an Auto Scaling group that uses automatic scaling.

Answer: B

Explanation:

- Scheduled scaling in ASG automatically increases capacity on known schedules with low overhead.

- Option A manual reminder is inefficient.

- Option C manual scaling requires human intervention.

- Option D automatic scaling isn't needed for predictable workloads.

Question 866:
A company is creating a REST API. The company has strict requirements for the use of TLS. The company requires TLSv1.3 on the API endpoints. The company also requires a specific public third-party certificate authority (CA) to sign the TLS certificate. Which solution will meet these requirements?

Options:
A.Use a local machine to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
B.Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
C.Use AWS Certificate Manager (ACM) to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
D.Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.

Answer: B

Explanation:

- Option B meets requirements because ACM can import a third-party CA signed certificate and API Gateway custom domains support TLSv1.3.

- Option A is unnecessary extra step since ACM directly supports importing third-party certificates.

- Option C Lambda function URLs do not support custom TLS CA in this scenario.

- Option D incorrect as Lambda URLs are not intended for this requirement.

Question 867:
A company runs an application on AWS. The application receives inconsistent amounts of usage. The application uses AWS Direct Connect to connect to an on-premises MySQL-compatible database. The on-premises database consistently uses a minimum of 2 GiB of memory. The company wants to migrate the on-premises database to a managed AWS service. The company wants to use auto scaling capabilities to manage unexpected workload increases. Which solution will meet these requirements with the LEAST administrative overhead?

Options:
A.Provision an Amazon DynamoDB database with default read and write capacity settings.
B.Provision an Amazon Aurora database with a minimum capacity of 1 Aurora capacity unit (ACU).
C.Provision an Amazon Aurora Serverless v2 database with a minimum capacity of 1 Aurora capacity unit (ACU).
D.Provision an Amazon RDS for MySQL database with 2 GiB of memory.

Answer: C

Explanation:

- Aurora Serverless v2 scales automatically up and down with usage, ideal for unpredictable workloads with low admin effort.

- Option A DynamoDB is NoSQL, incompatible with MySQL apps.

- Option B Aurora with fixed ACU still needs manual scaling.

- Option D RDS MySQL has fixed capacity, no auto scaling.

Question 868:
A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Configure Lambda provisioned concurrency.
B.Increase the timeout of the Lambda functions.
C.Increase the memory of the Lambda functions.
D.Configure Lambda SnapStart.

Answer: D

Explanation:

- Lambda SnapStart reduces Java function cold starts at no extra concurrency cost.

- Option A provisioned concurrency removes cold starts but is more expensive.

- Option B increasing timeout does not reduce latency.

- Option C increasing memory helps performance but not cold starts.

Question 869:
A financial services company launched a new application that uses an Amazon RDS for MySQL database. The company uses the application to track stock market trends. The company needs to operate the application for only 2 hours at the end of each week. The company needs to optimize the cost of running the database. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.
B.Migrate the existing RDS for MySQL database to an Aurora MySQL database cluster.
C.Migrate the existing RDS for MySQL database to an Amazon EC2 instance that runs MySQL. Purchase an instance reservation for the EC2 instance.
D.Migrate the existing RDS for MySQL database to an Amazon Elastic Container Service (Amazon ECS) cluster that uses MySQL container images to run tasks.

Answer: A

Explanation:

- Aurora Serverless v2 scales to zero when not in use, making it cost-effective for only 2 hours weekly usage.

- Option B Aurora MySQL incurs costs 24/7.

- Option C EC2 reserved instance wastes cost since DB runs only 2 hours weekly.
- Option D ECS adds management overhead and cost inefficiency.

Question 870:
A company deploys its applications on Amazon Elastic Kubernetes Service (Amazon EKS) behind an Application Load Balancer in an AWS Region. The application needs to store data in a PostgreSQL database engine. The company wants the data in the database to be highly available. The company also needs increased capacity for read workloads. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Create an Amazon DynamoDB database table configured with global tables.
B.Create an Amazon RDS database with Multi-AZ deployments.
C.Create an Amazon RDS database with Multi-AZ DB cluster deployment.
D.Create an Amazon RDS database configured with cross-Region read replicas.

Answer: C

Explanation:

- Multi-AZ DB cluster deployment provides high availability and supports read scaling with reader instances.
- Option A DynamoDB is NoSQL, not PostgreSQL.
- Option B Multi-AZ deployment provides HA but no read scaling.
- Option D cross-Region replicas increase cost and latency, not required.

Question 871:
A company is building a RESTful serverless web application on AWS by using Amazon API Gateway and AWS Lambda. The users of this web application will be geographically distributed, and the company wants to reduce the latency of API requests to these users. Which type of endpoint should a solutions architect use to meet these requirements?

Options:
A.Private endpoint
B.Regional endpoint
C.Interface VPC endpoint
D.Edge-optimized endpoint

Answer: D

Explanation:

- Edge-optimized endpoints leverage CloudFront to reduce latency for global users.
- Option A private endpoints restrict traffic to a VPC.
- Option B regional endpoints only serve traffic from one Region.
- Option C interface VPC endpoints are for private access inside VPCs, not global latency reduction.

Question 872:
A company uses an Amazon CloudFront distribution to serve content pages for its website. The company needs to ensure that clients use a TLS certificate when accessing the company's website. The company wants to automate the creation and renewal of the TLS certificates. Which solution will meet these requirements with the MOST operational efficiency?

Options:
A.Use a CloudFront security policy to create a certificate.
B.Use a CloudFront origin access control (OAC) to create a certificate.
C.Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain.
D.Use AWS Certificate Manager (ACM) to create a certificate. Use email validation for the domain.

Answer: C

Explanation:

- ACM with DNS validation automates renewal and integrates with CloudFront.

- Option A CloudFront policies don't issue certificates.

- Option B OAC manages access to origin, not TLS.

- Option D email validation requires manual approval, not fully automated.

Question 873:
A company deployed a serverless application that uses Amazon DynamoDB as a database layer. The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use DynamoDB Accelerator (DAX).
B.Migrate the database to Amazon Redshift.
C.Migrate the database to Amazon RDS.
D.Use Amazon ElastiCache for Redis.

Answer: A

Explanation:

- DAX provides microsecond read performance and is fully managed.

- Option B Redshift is for analytics, not transactional workloads.

- Option C RDS is not NoSQL and not suited for DynamoDB use case.

- Option D Redis caching works but requires additional logic and ops.

Question 874:
A company runs an application that uses Amazon RDS for PostgreSQL. The application receives traffic only on weekdays during business hours. The company wants to optimize costs and reduce operational overhead based on this usage. Which solution will meet these requirements?

Options:
A.Use the Instance Scheduler on AWS to configure start and stop schedules.
B.Turn off automatic backups. Create weekly manual snapshots of the database.
C.Create a custom AWS Lambda function to start and stop the database based on minimum CPU utilization.
D.Purchase All Upfront reserved DB instances.

Answer: A

Explanation:

- Instance Scheduler automates stopping/starting RDS based on schedule, cost-efficient.

- Option B backups don't address cost reduction.

- Option C custom Lambda increases overhead unnecessarily.

- Option D reserved instances run 24/7, wasting money.

Question 875:
A company uses locally attached storage to run a latency-sensitive application on premises. The company is using a lift and shift method to move the application to the AWS Cloud. The company does not want to change the application architecture. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for Lustre file system to run the application.
B.Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP2 volume to run the application.
C.Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for OpenZFS file system to run the application.
D.Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP3 volume to run the application.

Answer: D

Explanation:

- EBS gp3 is cost-effective, provides high performance, and matches locally attached storage.

- Option A FSx Lustre is for HPC workloads, costlier.

- Option B gp2 is older, more expensive than gp3.

- Option C FSx OpenZFS is more complex than required.

Question 876:

A company runs a stateful production application on Amazon EC2 instances. The application requires at least two EC2 instances to always be running. A solutions architect needs to design a highly available and fault-tolerant architecture for the application. The solutions architect creates an Auto Scaling group of EC2 instances. Which set of additional steps should the solutions architect take to meet these requirements?

Options:

A.Set the Auto Scaling group's minimum capacity to two. Deploy one On-Demand Instance in one Availability Zone and one On-Demand Instance in a second Availability Zone.

B.Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two On-Demand Instances in a second Availability Zone.

C.Set the Auto Scaling group's minimum capacity to two. Deploy four Spot Instances in one Availability Zone.

D.Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two Spot Instances in a second Availability Zone.

Answer: B

Explanation:

- Having two per AZ ensures HA and meets requirement of at least two running instances.

- Option A one per AZ risks losing AZ capacity.

- Option C Spot instances are not reliable for stateful workloads.

- Option D mixing Spot for stateful apps is risky.

Question 877:

An ecommerce company uses Amazon Route 53 as its DNS provider. The company hosts its website on premises and in the AWS Cloud. The company's on-premises data center is near the us-west-1 Region. The company uses the eu-central-1 Region to host the website. The company wants to minimize load time for the website as much as possible. Which solution will meet these requirements?

Options:

A.Set up a geolocation routing policy. Send the traffic that is near us-west-1 to the on-premises data center. Send the traffic that is near eu-central-1 to eu-central-1.

B.Set up a simple routing policy that routes all traffic that is near eu-central-1 to eu-central-1 and routes all traffic that is near the on-premises datacenter to the on-premises data center.

C.Set up a latency routing policy. Associate the policy with us-west-1.

D.Set up a weighted routing policy. Split the traffic evenly between eu-central-1 and the on-premises data center.

Answer: A

Explanation:

- Geolocation routing directs traffic based on user location, minimizing latency.

- Option B simple routing cannot route based on geography.

- Option C latency routing considers latency but not geography in this hybrid setup.

- Option D weighted routing doesn't optimize for latency or geography.

Question 878:
A company has 5 PB of archived data on physical tapes. The company needs to preserve the data on the tapes for another 10 years for compliance purposes. The company wants to migrate to AWS in the next 6 months. The data center that stores the tapes has a 1 Gbps uplink internet connectivity. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.
B.Use an on-premises backup application to read the data from the tapes and to write directly to Amazon S3 Glacier Deep Archive.
C.Order multiple AWS Snowball devices that have Tape Gateway. Copy the physical tapes to virtual tapes in Snowball. Ship the Snowball devices to AWS. Create a lifecycle policy to move the tapes to Amazon S3 Glacier Deep Archive.
D.Configure an on-premises Tape Gateway. Create virtual tapes in the AWS Cloud. Use backup software to copy the physical tape to the virtual tape.

Answer: C

Explanation:

- Snowball with Tape Gateway allows offline bulk transfer, cost-efficient and fast for PB-scale migration.

- Option A DataSync over 1 Gbps for 5 PB would take too long.

- Option B direct transfer over internet impractical at this scale.

- Option D Tape Gateway online transfer is too slow for PB data.

Question 879:
A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware. Which networking solution meets these requirements?

Options:
A.Run the EC2 instances in a spread placement group.
B.Group the EC2 instances in separate accounts.
C.Configure the EC2 instances with dedicated tenancy.
D.Configure the EC2 instances with shared tenancy.

Answer: A

Explanation:

- Spread placement group ensures instances are on separate hardware for resilience.

- Option B separate accounts doesn't guarantee separation of hardware.

- Option C dedicated tenancy ensures dedicated hardware but not separation across nodes.

- Option D shared tenancy is default, doesn't guarantee separation.

Question 880:
A solutions architect is designing a disaster recovery (DR) strategy to provide Amazon EC2 capacity in a failover AWS Region. Business requirements state that the DR strategy must meet capacity in the failover Region. Which solution will meet these requirements?

Options:
A.Purchase On-Demand Instances in the failover Region.
B.Purchase an EC2 Savings Plan in the failover Region.
C.Purchase regional Reserved Instances in the failover Region.
D.Purchase a Capacity Reservation in the failover Region.

Answer: D

Explanation:

- Capacity Reservation guarantees capacity availability in DR Region.

- Option A On-Demand cannot guarantee capacity during failover.

- Option B Savings Plans save cost but don't guarantee capacity.

- Option C Reserved Instances reserve pricing, not guaranteed capacity.

Question 881:
A company has five organizational units (OUs) as part of its organization in AWS Organizations. Each OU correlates to the five businesses that the company owns. The company's research and development (R&D) business is separating from the company and will need its own organization. A solutions architect creates a separate new management account for this purpose. What should the solutions architect do next in the new management account?

Options:
A.Have the R&D AWS account be part of both organizations during the transition.
B.Invite the R&D AWS account to be part of the new organization after the R&D AWS account has left the prior organization.
C.Create a new R&D AWS account in the new organization. Migrate resources from the prior R&D AWS account to the new R&D AWS account.
D.Have the R&D AWS account join the new organization. Make the new management account a member of the prior organization.

Answer: B

Explanation:

- Correct process is leaving old org first, then joining new one via invitation.

- Option A AWS account cannot belong to two orgs simultaneously.

- Option C creating new account requires full migration, more work.

- Option D management accounts cannot join other orgs.

Question 882:
A company is designing a solution to capture customer activity in different web applications to process analytics and make predictions. Customer activity in the web applications is unpredictable and can increase suddenly. The company requires a solution that integrates with other web applications. The solution must include an authorization step for security purposes. Which solution will meet these requirements?

Options:
A.Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives in an Amazon Elastic File System (Amazon EFS) file system. Authorization is resolved at the GWLB.
B.Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis data stream that stores the information that the company receives in an Amazon S3 bucket. Use an AWS Lambda function to resolve authorization.
C.Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.
D.Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives on an Amazon Elastic File System (Amazon EFS) file system. Use an AWS Lambda function to resolve authorization.

Answer: C

Explanation:

- API Gateway + Kinesis Data Firehose + Lambda authorizer provides event-driven ingestion with built-in authorization.

- Option A GWLB not intended for app-level authorization.

- Option B Kinesis data stream requires additional coding to handle auth properly.

- Option D GWLB not suitable for security authorization flow.

Question 883:
An ecommerce company wants a disaster recovery solution for its Amazon RDS DB instances that run Microsoft SQL Server Enterprise Edition. The company's current recovery point objective (RPO) and recovery time objective (RTO) are 24 hours. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Create a cross-Region read replica and promote the read replica to the primary instance.
B.Use AWS Database Migration Service (AWS DMS) to create RDS cross-Region replication.
C.Use cross-Region replication every 24 hours to copy native backups to an Amazon S3 bucket.
D.Copy automatic snapshots to another Region every 24 hours.

Answer: D

Explanation:

- Copying automatic snapshots to another Region daily meets 24h RPO/RTO at lowest cost.

- Option A read replica adds cost and provides near real-time RPO.

- Option B DMS replication is continuous, more costly.

- Option C native backup replication adds management overhead.

Question 884:
A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer that has sticky sessions enabled. The web server currently hosts the user session state. The company wants to ensure high availability and avoid user session state loss in the event of a web server outage. Which solution will meet these requirements?

Options:
A.Use an Amazon ElastiCache for Memcached instance to store the session data. Update the application to use ElastiCache for Memcached to store the session state.
B.Use Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state.
C.Use an AWS Storage Gateway cached volume to store session data. Update the application to use AWS Storage Gateway cached volume to store the session state.
D.Use Amazon RDS to store the session state. Update the application to use Amazon RDS to store the session state.

Answer: B

Explanation:

- ElastiCache Redis is ideal for session storage with persistence and HA.

- Option A Memcached lacks persistence, less reliable.

- Option C Storage Gateway not designed for session data.

- Option D RDS adds latency and is overkill for session state.

Question 885:
A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads. Which solution will meet these requirements?

Options:
A.Create a read replica of the database. Direct the queries to the read replica.
B.Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.
C.Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.
D.Resize the DB instance to accommodate the additional workload.

Answer: A

Explanation:

- Read replica offloads reporting workload from primary DB without impacting performance.

- Option B backup + restore adds delay and management.

- Option C Athena requires exporting data, not real-time.

- Option D resizing for one-time workload is wasteful.

Question 886:
A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices. Which solution will meet this requirement MOST cost-effectively?

Options:
A.Use the AWS Load Balancer Controller to provision a Network Load Balancer.
B.Use the AWS Load Balancer Controller to provision an Application Load Balancer.
C.Use an AWS Lambda function to connect the requests to Amazon EKS.
D.Use Amazon API Gateway to connect the requests to Amazon EKS.

Answer: B

Explanation:

- ALB with AWS Load Balancer Controller is cost-effective and integrates with Kubernetes ingress for routing microservices.

- Option A NLB works at TCP/Layer 4, not for routing HTTP-based microservices.

- Option C Lambda adds unnecessary cost and overhead.

- Option D API Gateway adds cost overhead and not needed for internal EKS microservices.

Question 887:
A company uses AWS and sells access to copyrighted images. The company's global customer base needs to be able to access these images quickly. The company must deny access to users from specific countries. The company wants to minimize costs as much as possible. Which solution will meet these requirements?

Options:
A.Use Amazon S3 to store the images. Turn on multi-factor authentication (MFA) and public bucket access. Provide customers with a link to the S3 bucket.
B.Use Amazon S3 to store the images. Create an IAM user for each customer. Add the users to a group that has permission to access the S3 bucket.
C.Use Amazon EC2 instances that are behind Application Load Balancers (ALBs) to store the images. Deploy the instances only in the countries the company services. Provide customers with links to the ALBs for their specific country's instances.
D.Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

Answer: D

Explanation:

- S3 + CloudFront with geo restrictions + signed URLs ensures fast delivery, secure and cost-effective.

- Option A public bucket insecure.

- Option B IAM users for each customer not scalable.

- Option C EC2 storage costly and inefficient.

Question 888:
A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level. Which solution will meet these requirements?

Options:
A.Use Multi-AZ Redis replication groups with shards that contain multiple nodes.
B.Use Redis shards that contain multiple nodes with Redis append only files (AOF) turned on.
C.Use a Multi-AZ Redis cluster with more than one read replica in the replication group.
D.Use Redis shards that contain multiple nodes with Auto Scaling turned on.

Answer: A

Explanation:

- Multi-AZ Redis replication groups with multiple nodes ensure HA at node and Region level.

- Option B AOF persistence ensures durability but not full HA.

- Option C Multi-AZ with replicas helps but doesn't guarantee shard-level scaling.

- Option D Auto Scaling doesn't solve HA requirements.

Question 889:
A company plans to migrate to AWS and use Amazon EC2 On-Demand Instances for its application. During the migration testing phase, a technical team observes that the application takes a long time to launch and load memory to become fully productive. Which solution will reduce the launch time of the application during the next testing phase?

Options:
A.Launch two or more EC2 On-Demand Instances. Turn on auto scaling features and make the EC2 On-Demand Instances available during the next testing phase.
B.Launch EC2 Spot Instances to support the application and to scale the application so it is available during the next testing phase.
C.Launch the EC2 On-Demand Instances with hibernation turned on. Configure EC2 Auto Scaling warm pools during the next testing phase.
D.Launch EC2 On-Demand Instances with Capacity Reservations. Start additional EC2 instances during the next testing phase.

Answer: C

Explanation:

- Hibernation + warm pools reduces startup time by keeping memory loaded and instances pre-warmed.

- Option A scaling doesn't reduce startup latency.

- Option B Spot doesn't solve startup latency and is unreliable.

- Option D Capacity Reservation ensures capacity but doesn't address long boot time.

Question 890:
A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week. The company wants to maintain application performance during sudden traffic increases. Which solution will meet these requirements MOST cost-effectively?

Options:
A.Use manual scaling to change the size of the Auto Scaling group.
B.Use predictive scaling to change the size of the Auto Scaling group.
C.Use dynamic scaling to change the size of the Auto Scaling group.
D.Use schedule scaling to change the size of the Auto Scaling group.

Answer: C

Explanation:

- Dynamic scaling automatically responds to real-time demand spikes, cost-efficient.

- Option A manual scaling is reactive and inefficient.

- Option B predictive scaling better for predictable patterns, not random spikes.

- Option D scheduled scaling doesn't help with unpredictable increases.

Question 891:
An ecommerce application uses a PostgreSQL database that runs on an Amazon EC2 instance. During a monthly sales event, database usage increases and causes database connection issues for the application. The traffic is unpredictable for subsequent monthly sales events, which impacts the sales forecast. The company needs to maintain performance when there is an unpredictable increase in traffic. Which solution resolves this issue in the MOST cost-effective way?

Options:
A.Migrate the PostgreSQL database to Amazon Aurora Serverless v2.
B.Enable auto scaling for the PostgreSQL database on the EC2 instance to accommodate increased usage.
C.Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a larger instance type.
D.Migrate the PostgreSQL database to Amazon Redshift to accommodate increased usage.

Answer: A

Explanation:

- Aurora Serverless v2 scales automatically and cost-effectively for unpredictable spikes.

- Option B EC2 cannot auto scale DB easily.

- Option C RDS with larger instance is expensive and static.

- Option D Redshift is for analytics, not transactional workloads.

Question 892:
A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency. Which solution will meet these requirements?

Options:
A.Increase the API Gateway throttling limit.
B.Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.
C.Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.
D.Increase the Lambda function memory.

Answer: B

Explanation:

- Provisioned concurrency pre-warms Lambda instances, reducing latency spikes at start of day.

- Option A throttling doesn't reduce cold starts.

- Option C CloudWatch alarm adds complexity, not effective for latency.

- Option D memory improves performance but not cold start latency.

Question 893:
A research company uses on-premises devices to generate data for analysis. The company wants to use the AWS Cloud to analyze the data. The devices generate .csv files and support writing the data to an SMB file share. Company analysts must be able to use SQL commands to query the data. The analysts will run queries periodically throughout the day. Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

Options:
A.Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.
B.Deploy an AWS Storage Gateway on premises in Amazon FSx File Gateway mode.
C.Set up an AWS Glue crawler to create a table based on the data that is in Amazon S3.
D.Set up an Amazon EMR cluster with EMR File System (EMRFS) to query the data that is in Amazon S3. Provide access to analysts.
E.Set up an Amazon Redshift cluster to query the data that is in Amazon S3. Provide access to analysts.
F.Setup Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Answer: A, C, F

Explanation:

- File Gateway pushes .csv to S3, Glue crawler creates schema, Athena queries using SQL, cost-efficient.

- Option B FSx File Gateway unnecessary.

- Option D EMR cluster expensive for periodic queries.

- Option E Redshift cluster costly for sporadic analysis.

Question 894:
A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes. A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application. Which activities are the responsibility of the company's operational team? (Choose three.)

Options:
A.Providing resilient power and network connectivity to the Outposts racks
B.Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts
C.Physical security and access controls of the data center environment
D.Availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the Outposts racks
E.Physical maintenance of Outposts components
F.Providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events

Answer: A, C, E

Explanation:

- Customer responsibility: resilient power/network, physical security, physical maintenance.

- Option B AWS manages hypervisor/storage/services.

- Option D AWS ensures availability of Outposts hardware.

- Option F AWS manages ECS scaling, not customer.

Question 895:
A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS. What should a solutions architect recommend to meet this requirement?

Options:
A.Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
B.Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
C.Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
D.Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Answer: A

Explanation:

- NLB handles millions of requests/sec at Layer 4 with low latency.

- Option B ALB is Layer 7 and cannot handle such scale at TCP.

- Option C CloudFront not suited for raw TCP traffic.

- Option D API Gateway is HTTP-based, not suitable for raw TCP high throughput.

Question 896:
A company has a global web application with unpredictable traffic. The company wants to minimize costs while ensuring high availability. Which AWS service combination should the company use?

Options:
A.Use Amazon Route 53 latency-based routing with Amazon CloudFront and Amazon S3.
B.Use Amazon API Gateway with AWS Lambda across multiple Regions.
C.Use Amazon Elastic Load Balancer with Auto Scaling groups across multiple Regions.
D.Use AWS Direct Connect with on-premises failover to AWS Regions.

Answer: A

Explanation:

- Route 53 + CloudFront + S3 ensures global distribution, high availability, and low cost.

- Option B Lambda multi-Region is more costly.

- Option C Multi-Region ELB/ASG adds higher cost and complexity.

- Option D Direct Connect is unnecessary for global web app.

Question 897:
A company needs secure communication between its on-premises network and its VPC. The company requires encryption in transit and cost-effectiveness. Which AWS service should the solutions architect recommend?

Options:
A.AWS Direct Connect without encryption
B.AWS Direct Connect with MACsec
C.AWS Site-to-Site VPN
D.AWS Global Accelerator

Answer: C

Explanation:

- Site-to-Site VPN provides encrypted IPsec tunnels over internet, cost-effective.

- Option A Direct Connect without encryption doesn't meet requirement.

- Option B Direct Connect with MACsec provides encryption but expensive.

- Option D Global Accelerator is for routing optimization, not encryption.

Question 898:
A company needs to migrate a large volume of log files from its on-premises data center to Amazon S3. The company has limited bandwidth and needs to complete the transfer within days. Which solution is MOST cost-effective?

Options:
A.Use AWS DataSync over internet.
B.Use AWS Snowball Edge device.
C.Use AWS Transfer Family with FTP.
D.Use AWS Storage Gateway file gateway.

Answer: B

Explanation:

- Snowball Edge is best for large-scale data migration with limited bandwidth.

- Option A DataSync over limited bandwidth is too slow.

- Option C Transfer Family is for FTP transfer, not bulk migration.

- Option D File Gateway is hybrid storage, not for large one-time migration.

Question 899:
A company has a real-time gaming application that requires sub-millisecond latency for frequently accessed data. The application must support millions of players worldwide. Which solution will meet these requirements?

Options:
A.Amazon Aurora Global Database
B.Amazon ElastiCache for Redis with Global Datastore
C.Amazon RDS Multi-AZ
D.Amazon S3 with Amazon CloudFront

Answer: B

Explanation:

- ElastiCache Redis Global Datastore supports sub-ms latency globally.

- Option A Aurora Global Database latency is in ms range.

- Option C RDS Multi-AZ for durability, not global sub-ms access.

- Option D S3 + CloudFront caching not suitable for transactional gaming data.

Question 900:

A company has a compliance requirement to encrypt all data stored in Amazon S3 using a customer managed key. The company must rotate the key annually. Which solution will meet these requirements with the LEAST operational overhead?

Options:
A.Use SSE-S3 (Amazon S3-managed keys).
B.Use SSE-KMS with AWS-managed keys (aws/s3).
C.Use SSE-KMS with a customer managed key. Enable automatic key rotation in KMS.
D.Encrypt objects on the client-side before uploading.

Answer: C

Explanation:

- Customer managed KMS keys with automatic rotation meets compliance with minimal effort.

- Option A SSE-S3 doesn't use customer managed keys.

- Option B AWS-managed keys don't meet customer managed requirement.

- Option D client-side encryption adds unnecessary complexity.

Question: 901

A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.
The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.
Which AWS solution will meet these requirements?

Options:
A. AWS Snowcone
B. Amazon FSx File Gateway
C. AWS DataSync
D. AWS Transfer Family

Answer: C

Explanation:

- A: Too small for 30 TB.

- B: Provides SMB access but not optimized migration.

- C: Correct, supports bandwidth throttling and fast transfers.

- D: Meant for SFTP/FTP transfers.

Question: 902

A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.

Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.

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

Options:

A. Deploy Amazon CloudFront for content delivery and caching.
B. Use AWS DataSync to replicate the video files across AWS Regions in other S3 buckets.
C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.
D. Deploy an Auto Scaling group of Amazon EC2 instances in Local Zones for content delivery and caching.
E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats.

Answer: AC

Explanation:

- A: Correct, improves performance globally.

- B: Incorrect, replication doesn't solve buffering.

- C: Correct, converts into device-optimized formats.

- D: Incorrect, adds complexity.

- E: Incorrect, managed transcoding is better.

Question: 903

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

Options:

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Answer: D

Explanation:

- A: ECS on Fargate cannot scale using EC2 Auto Scaling.

- B: Unnecessary complexity.

- C: Incorrect, EC2-specific scaling.

- D: Correct, native ECS scaling with Application Auto Scaling.

Question: 904

A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.

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

Options:

A. Use AWS DataSync.
B. Use AWS Snowball devices.
C. Set up an SFTP server on Amazon EC2.
D. Use AWS Database Migration Service (AWS DMS).

Answer: A

Explanation:

- A: Correct, DataSync supports cross-Region NFS transfers.

- B: Snowball is for one-time bulk transfers.

- C: Requires maintenance.

- D: For databases, not file systems.

Question: 905

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

Options:

A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
C. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.
D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

Answer: C

Explanation:

- A: DataSync is for transfers, not SMB hosting.

- B: Adds operational burden.

- C: Correct, FSx for Windows is managed SMB.

- D: S3 is object storage, not SMB.

Question: 906

A company that primarily runs its application servers on premises has decided to migrate to AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

Options:

A. Amazon S3 File Gateway

B. AWS Storage Gateway Tape Gateway

C. AWS Storage Gateway Volume Gateway stored volumes

D. AWS Storage Gateway Volume Gateway cached volumes

Answer: D

Explanation:

- A: File Gateway is for SMB/NFS to S3, not iSCSI.

- B: Tape Gateway is for backup tapes.

- C: Stored volumes keep all data on-premises.

- D: Correct, cached volumes keep recent data local.

Question: 907

A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

Which combination of steps should the finance team take to meet these requirements? (Choose two.)

Options:

A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.

B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.

C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.

D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.

E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.

Answer: BD

Explanation:

- A: Incorrect, must use consolidated billing view.

- B: Correct, consolidated billing sees all usage.

- C: Reserved optimization isn't enough alone.

- D: Correct, Idle DB Instances highlights savings.

- E: Irrelevant to RDS Oracle.

Question: 908

A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.
Which solution will accomplish this goal with the LEAST operational overhead?

Options:
A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.
B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.
C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.
D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.

Answer: A

Explanation:

- A: Correct, Storage Lens provides usage patterns with least effort.

- B: Console dashboard lacks deep metrics.

- C: Bucket size doesn't show access frequency.

- D: CloudTrail tracks API calls, not detailed usage trends.

Question: 909

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.
The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.
What should a solutions architect do to meet these requirements?

Options:
A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.
B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.
C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.
D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

Answer: B

Explanation:

- A: Increases performance but higher cost.

- B: Correct, CloudFront reduces transfer cost and latency.

- C: More management overhead, not cost optimized.

- D: Requires application rework.

Question: 910
A company is using AWS to design a web application that will process insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost. The solution must maximize operational efficiency and must minimize maintenance.
Which solution meets these requirements?

Options:
A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pool messages from its own data stream.
B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type. Subscribe the Lambda function to its associated SNS topic. Configure the application to publish requests for quotes to the appropriate SNS topic.
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to use its own SQS queue.
D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon OpenSearch Service cluster. Configure the application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from OpenSearch Service and process them accordingly.

Answer: C

Explanation:

- A: Overhead with multiple Kinesis streams.

- B: SNS alone doesn't guarantee persistence.

- C: Correct, SNS with SQS + filtering ensures reliable, separated delivery.

- D: Overkill with Firehose + OpenSearch.

Question: 911
A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.
Which solution will meet these requirements in the MOST operationally efficient way?

Options:
A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.
B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EC2 instances as resources.
C. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EBS volumes as resources.
D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone.

Answer: B

Explanation:

- A: Custom Lambda adds management.

- B: Correct, AWS Backup handles scheduling + cross-Region copies.

- C: Possible, but using EC2 instance resources covers config + volumes.

- D: AZ snapshots don't provide Region-level recovery.

Question: 912
A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.
What should a solutions architect recommend to meet these requirements?

Options:
A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
C. Use Amazon CloudFront. Provide signed URLs to stream content.
D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer: C

Explanation:

- A: Public bucket violates security.

- B: VPN not suitable for millions of mobile users.

- C: Correct, CloudFront signed URLs secure + scale.

- D: Client VPN is not for streaming.

Question: 913

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.
Which service should a solutions architect recommend?

Options:

A. Amazon Aurora MySQL
B. Amazon Aurora Serverless for MySQL
C. Amazon Redshift Spectrum
D. Amazon RDS for MySQL

Answer: B

Explanation:

- A: Aurora requires choosing instance sizes.

- B: Correct, Aurora Serverless scales automatically, no instance selection.

- C: Redshift Spectrum is for analytics, not OLTP.

- D: RDS requires instance sizing.

Question: 914

A company experienced a breach that affected several applications in its on-premises data center. The attacker took advantage of vulnerabilities in the custom applications that were running on the servers. The company is now migrating its applications to run on Amazon EC2 instances. The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings.
Which solution will meet these requirements?

Options:

A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities. Create an AWS Lambda function to log any findings to AWS CloudTrail.
B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities. Log any findings to AWS CloudTrail.
C. Turn on Amazon GuardDuty. Deploy the GuardDuty agents to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
D. Turn on Amazon Inspector. Deploy the Amazon Inspector agent to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.

Answer: D

Explanation:

- A: Shield is for DDoS protection.

- B: Macie is for data classification.

- C: GuardDuty detects threats but doesn't scan instances.

- D: Correct, Inspector scans for vulnerabilities.

Question: 915

A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.

What should a solutions architect recommend to meet these requirements?

Options:

A. Increase the size of the EC2 instance to process messages faster.

B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.

C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate runtime.

D. Use AWS Systems Manager Run Command to run the script on demand.

Answer: C

Explanation:

- A: Larger EC2 increases costs.

- B: EventBridge won't scale dynamically.

- C: Correct, Lambda scales automatically with queue size.

- D: Manual trigger doesn't solve scaling.

Question: 916

A company uses a legacy application to produce data in CSV format. The legacy application stores the output data in Amazon S3. The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored in Amazon Redshift and Amazon S3 only. However, the COTS application cannot process the .csv files that the legacy application produces.

The company cannot update the legacy application to produce data in another format. The company needs to implement a solution so that the COTS application can use the data that the legacy application produces.

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

Options:

A. Create an AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshift.

B. Develop a Python script that runs on Amazon EC2 instances to convert the .csv files to .sql files. Invoke the Python script on a cron schedule to store the output files in Amazon S3.

C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.

D. Use Amazon EventBridge to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

Answer: A

Explanation:

- A: Correct, Glue ETL converts CSV to Redshift-friendly format easily.

- B: Manual EC2 adds management overhead.

- C: DynamoDB doesn't support SQL queries.

- D: EMR is too heavy for simple conversion.

Question: 917
A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must devise a strategy to track and audit these inventory and configuration changes.
Which actions should the solutions architect take to meet these requirements? (Choose two.)

Options:
A. Enable AWS CloudTrail and use it for auditing.
B. Use data lifecycle policies for the Amazon EC2 instances.
C. Enable AWS Trusted Advisor and reference the security dashboard.
D. Enable AWS Config and create rules for auditing and compliance purposes.
E. Restore previous resource configurations with an AWS CloudFormation template.

Answer: AD

Explanation:

- A: Correct, CloudTrail tracks API calls.

- B: Not related to auditing.

- C: Trusted Advisor provides recommendations, not change tracking.

- D: Correct, Config tracks configuration changes.

- E: Not part of monitoring/auditing.

Question: 918
A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.
Which solution will meet this requirement with the LEAST amount of administrative overhead?

Options:
A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Answer: A

Explanation:

- A: Correct, Session Manager allows secure, keyless access.

- B: Adds custom management.

- C: Still relies on SSH keys.

- D: Overly complex for SSH.

Question: 919

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

Options:

A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Answer: A

Explanation:

- A: Correct, Kinesis Data Streams provides durable ingestion + near real-time querying.

- B: Firehose to Redshift adds latency.

- C: Instance store loses data on reboot.

- D: Redis not suitable for durable ingestion at scale.

Question: 920

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

Options:

A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Answer: D

Explanation:

- A: ACL header doesn't enforce encryption.

- B: Private ACL doesn't mean encryption.

- C: SecureTransport enforces HTTPS, not encryption at rest.

- D: Correct, SSE header ensures encryption.

Question: 921
A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.
The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.
What should the solutions architect do to meet these requirements?

Options:
A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
B. Create an AWS Step Functions workflow. Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.
C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.
D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions. Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Answer: C

Explanation:

- A: Would delay user response until thumbnail is complete.

- B: Adds complexity and delays response.

- C: Correct, SQS decouples processing and provides fast acknowledgment.

- D: SNS alone doesn't queue reliably for long jobs.

Question: 922

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

Options:

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.

B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.

D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B

Explanation:

- A: Single EC2 introduces SPOF.

- B: Correct, API Gateway + Lambda + DynamoDB is fully managed and scalable.

- C: Route 53 cannot directly receive HTTPS requests.

- D: VPN to S3 is not scalable for HTTPS badge events.

Question: 923

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

Options:

A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.

B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.

C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Answer: D

Explanation:

- A: Requires NFS change, not minimal.

- B: Tape Gateway unsuitable for live access.

- C: Cached volume stores most data in cloud, not local.

- D: Correct, stored volume keeps all data local + DR snapshots.

Question: 924
A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket.
Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.
Which solution meets these requirements?

Options:
A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.
B. Update the S3 ACL to allow the application to access the protected content.
C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.
D. Update the Amazon Cognito pool to use custom attribute mappings within the identity pool and grant users the proper permissions to access the protected content.

Answer: A

Explanation:

- A: Correct, Cognito must assume IAM role with permissions.

- B: ACLs don't integrate with Cognito.

- C: Eventual consistency not the issue.

- D: Custom mappings not required here.

Question: 925
An image hosting company uploads its large assets to Amazon S3 Standard buckets. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.
Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)

Options:
A. Move assets to S3 Intelligent-Tiering after 30 days.
B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.
C. Configure an S3 Lifecycle policy to clean up expired object delete markers.
D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: AB

Explanation:

- A: Correct, Intelligent-Tiering adapts to unpredictable access.

- B: Correct, cleaning incomplete uploads saves costs.

- C: Expired delete markers irrelevant.

- D: Not optimal with inconsistent access.

- E: One Zone-IA sacrifices resiliency.

Question: 926
A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.
Which solution meets these requirements?

Options:
A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall firewall. Configure domain list rule groups.
B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct all outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.

Answer: A

Explanation:

- A: Correct, Network Firewall supports domain filtering.

- B: WAF protects web apps, not outbound traffic.

- C: Security groups can't filter by URL.

- D: ALB is for inbound traffic.

Question: 927
A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.
The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.
What should a solutions architect recommend to ensure that all the requests are processed successfully?

Options:
A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Answer: D

Explanation:

- A: CloudFront on dynamic content not ideal.

- B: Scaling EC2 is not sufficient for async processing.

- C: ElastiCache doesn't solve async backlog.

- D: Correct, SQS ensures all requests are queued + processed.

Question: 928
A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.
Which solution will meet these requirements?

Options:
A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.
B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.
C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.
D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.

Answer: D

Explanation:

- A: Macie is for sensitive data discovery.

- B: GuardDuty detects threats, not patching.

- C: Detective investigates incidents, not scanning/patching.

- D: Correct, Inspector + Systems Manager covers both scanning + patching.

Question: 929
A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.
What should a solutions architect do to meet this requirement?

Options:
A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.
B. Create an encryption key. Store the key in AWS Secrets Manager. Use the key to encrypt the DB instances.
C. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate.
D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate.

Answer: A

Explanation:

- A: Correct, RDS uses KMS keys for encryption at rest.

- B: Secrets Manager is not for at-rest DB encryption.

- C/D: Certificates apply to in-transit encryption.

Question: 930

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization.
What should a solutions architect do to meet these requirements?

Options:

A. Use AWS Snowball.
B. Use AWS DataSync.
C. Use a secure VPN connection.
D. Use Amazon S3 Transfer Acceleration.

Answer: A

Explanation:

- A: Correct, Snowball is ideal for large data with bandwidth limits.

- B: DataSync over limited bandwidth won't meet 30 days.

- C: VPN doesn't solve transfer speed.

- D: Transfer Acceleration still limited by bandwidth.

Question: 931
A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

Options:
A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

Answer: B

Explanation:

- A: Public EC2 introduces risk.

- B: Correct, FSx integrates with AD + secure VPN.

- C: Signed URL may not enforce corporate auth.

- D: Public endpoint is insecure.

Question: 932
A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch runs. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

Options:
A. Configure an Amazon CloudFront distribution in front of the ALB.
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Answer: C

Explanation:

- A: CloudFront doesn't solve compute-heavy jobs.

- B: Scaling reacts too late to sudden CPU spikes.

- C: Correct, scheduled scaling anticipates monthly workload.

- D: ElastiCache won't help batch jobs.

Question: 933
A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.
Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

Options:
A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.
B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.
C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).
D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

Answer: A

Explanation:

- A: Correct, Transfer Family supports SFTP + AD auth.

- B: DMS is for databases.

- C: DataSync doesn't expose SFTP.

- D: EC2 adds management overhead.

Question: 934
A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.
Which solution meets these requirements?

Options:
A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.
B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.
C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.
D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs. Configure Auto Scaling group capacity limits as an event source in EventBridge.

Answer: B

Explanation:

- A: Manual and slow.

- B: Correct, FSR ensures faster initialization from AMIs.

- C: Lifecycle Manager not real-time.

- D: Backup lifecycle irrelevant.

Question: 935

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days. What should a solutions architect do to meet this requirement with the LEAST operational effort?

Options:

A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.

B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.

C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.

D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Answer: A

Explanation:

- A: Correct, Secrets Manager automates secure storage and rotation.

- B: More manual effort than Secrets Manager.

- C: EFS adds unnecessary complexity.

- D: S3 adds manual management.

Question: 936

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

Options:

A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.

B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.

C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.

D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Answer: A

Explanation:

- A: Correct, Aurora provides near real-time replication + scaling.

- B: Adds code changes + caching, doesn't solve replica lag.

- C: High overhead managing MySQL on EC2.

- D: DynamoDB is a different model, large changes required.

Question: 937

A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replicate data to a secondary AWS Region.

Which solution will meet these requirements MOST cost-effectively?

Options:

A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.

B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.

C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.

D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

Answer: D

Explanation:

- A: Binary log replication is more manual and costly.

- B: Aurora global DB requires at least one DB instance.

- C: DMS not efficient for ongoing DR replication.

- D: Correct, Aurora global DB ensures replication across Regions cost-effectively.

Question: 938
A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.
What should a solutions architect do to meet these requirements?

Options:
A. Use AWS Key Management Service (AWS KMS) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: C

Explanation:

- A: KMS doesn't manage credentials.

- B: Lambda adds unnecessary management.

- C: Correct, Secrets Manager automates credential rotation.

- D: Parameter Store rotation not native like Secrets Manager.

Question: 939

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

Options:

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
B. Create an ALB listener rule to reply to SQL injections with a fixed response.
C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
D. Set up Amazon Inspector to block all SQL injection attempts automatically.

Answer: A

Explanation:

- A: Correct, WAF prevents SQL injection.

- B: Listener rules cannot filter SQL injection.

- C: Shield Advanced is for DDoS, not SQLi.

- D: Inspector scans for vulnerabilities, not block attacks.

Question: 940

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

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

Options:

A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.
D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

Answer: D

Explanation:

- A: Requires manual ingestion + lacks column-level auth.

- B: IAM policies cannot enforce column-level rules.

- C: Glue Elastic Views lacks direct column-level auth integration.

- D: Correct, Lake Formation handles fine-grained access.

Question: 941

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run. Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity. Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.

B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.

C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.

D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Answer: C

Explanation:

- A: Reactive scaling will not provision early.

- B: Works, but predictive scaling is smarter.

- C: Correct, predictive scaling launches capacity in advance.

- D: Triggering at 60% is too late.

Question: 942

A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.
Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Answer: C

Explanation:

- A: High overhead on EC2.

- B: Multi-AZ doesn't cover cross-Region.

- C: Correct, Aurora global DB supports cross-Region replication.

- D: CRR backups restore manually, not immediate DR.

Question: 943

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.
Which solution will meet these requirements with the FEWEST changes to the code?

Options:

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.
C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.
D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

Answer: A

Explanation:

- A: Correct, Extended Client Library allows storing large messages in S3.

- B: EventBridge doesn't solve large payloads easily.

- C: SQS has fixed limit, cannot change.

- D: EFS not integrated with SQS.

Question: 944

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

Options:

A. Use Amazon Cognito for authentication. Use for authorization. Use Amazon CloudFront to serve the web application globally.

B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.

C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.

D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Answer: A

Explanation:

- A: Correct, Cognito + CloudFront + Lambda@Edge gives low latency + scalability.

- B: AD is overkill for <100 users.

- C: S3 Transfer Acceleration doesn't handle global delivery.

- D: Elastic Beanstalk adds cost and complexity.

Question: 945

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

Options:
A. Volume Gateway
B. Tape Gateway
C. Amazon FSx File Gateway
D. Amazon S3 File Gateway

Answer: D

Explanation:

- A: Volume Gateway presents iSCSI, not SMB/NFS.

- B: Tape Gateway is for backup.

- C: FSx File Gateway is not an AWS service.

- D: Correct, S3 File Gateway presents SMB/NFS backed by S3.

Question: 946

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company. The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

Options:

A. Compute Savings Plan
B. EC2 Instance Savings Plan
C. Zonal Reserved Instances
D. Standard Reserved Instances

Answer: A

Explanation:

- A: Correct, Compute Savings Plans allow flexibility in instance family + Region.

- B: Instance SP locks to family.

- C: Zonal RIs lack flexibility.

- D: Standard RIs are restrictive.

Question: 947

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Which solution will meet these requirements MOST cost-effectively?

Options:

A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Answer: B

Explanation:

- A: Standard-IA applies to S3, not DynamoDB.

- B: Correct, provisioned mode with steady workload is cost-effective.

- C: On-demand is more expensive for predictable workloads.

- D: On-demand doesn't support reserved capacity.

Question: 949

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.
What should a solutions architect do to meet these requirements?

Options:

A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.

B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.

D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

Answer: B

Explanation:

- A: Creating an unencrypted snapshot weakens security.

- B: Correct, encrypted snapshots require key access. Adding the acquiring company to the KMS key policy allows secure sharing.

- C: Cannot re-encrypt with AWS-managed keys for sharing.

- D: Downloading/uploading snapshots is not secure or supported for RDS.

Question: 950

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance. The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.
Which combination of steps will meet these requirements? (Choose two.)

Options:

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.

B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.

C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.

D. Migrate the database to RDS Custom.

E. Use RDS Proxy to limit reporting requests to the maintenance window.

Answer: AC

Explanation:

- A: Multi-AZ provides high availability and automatic failover.

- B: Restoring a snapshot is manual, not a continuous solution.

- C: Correct, read replicas reduce load from reporting queries.

- D: RDS Custom is not needed here.

- E: RDS Proxy improves connection handling, but not reporting load.

Question: 951

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.
Which solution will meet these requirements?

Options:

A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.

B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.

C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.

D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Answer: D

Explanation:

- A: Glue is for ETL, not full event-driven workflow orchestration.

- B: EC2 adds management overhead, not serverless.

- C: EventBridge schedules events but doesn't manage workflow state.

- D: Correct, Step Functions + Lambda = serverless, event-driven, minimal overhead.

Question: 952

A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.
Which solution will meet these requirements?

Options:

A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.

B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.

C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.

D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Answer: B

Explanation:

- A: Transit gateway adds latency and is not global optimized.

- B: Correct, Global Accelerator supports UDP, optimizes routing, improves latency.

- C: CloudFront does not support UDP.

- D: VPC peering does not help with global latency.

Question: 953

A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

Options:

A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.

B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.

C. Use Amazon S3 Intelligent-Tiering access tiers.

D. Use two large EC2 instances to host the database in active-passive mode.

Answer: B

Explanation:

- A: io2 is over-provisioned and more expensive.

- B: Correct, RDS Multi-AZ with gp2 provides high availability + cost efficiency.

- C: S3 Intelligent-Tiering not applicable for relational databases.

- D: EC2 self-management adds complexity.

Question: 954

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

Options:

A. Reduce the Lambda concurrency rate.

B. Enable RDS Proxy on the RDS DB instance.

C. Resize the RDS DB instance class to accept more connections.

D. Migrate the database to Amazon DynamoDB with on-demand scaling.

Answer: B

Explanation:

- A: Reducing concurrency throttles workload.

- B: Correct, RDS Proxy pools DB connections, prevents timeouts.

- C: Upsizing DB is costly and not efficient.

- D: DynamoDB migration requires major app changes.

Question: 955

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

Options:

A. Use AWS Lambda with functional scaling.

B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.

C. Use Amazon Lightsail with AWS Auto Scaling.

D. Use AWS Batch on Amazon EC2.

Answer: D

Explanation:

- A: Lambda has runtime and resource limits.

- B: Fargate not ideal for large batch jobs needing 64 vCPUs.

- C: Lightsail is for simple apps, not HPC workloads.

- D: Correct, AWS Batch manages compute for heavy batch jobs.

Question: 956

A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.

Which storage solution will meet these requirements?

Options:

A. Move the data objects to S3 Glacier Deep Archive after 30 days.

B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Answer: B

Explanation:

- A: Glacier Deep Archive not immediately accessible.

- B: Correct, S3 Standard-IA provides same durability + lower cost.

- C: One Zone-IA lacks multi-AZ resiliency.

- D: Immediate move risks high cost for frequent access.

Question: 957

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

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

Options:
A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Answer: AD

Explanation:

- A: Correct, S3 + CloudFront provides scalable static hosting.

- B: ElastiCache is for DB queries, not static file hosting.

- C: EFS is POSIX-compliant, but Windows app requires FSx.

- D: Correct, FSx for Windows supports Windows shared storage.

- E: EBS cannot be shared across multiple EC2 instances.

Question: 958
A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.
Which solution will meet these requirements with the LEAST operational overhead?

Options:
A. Install an external image management library on an EC2 instance. Use the image management library to process the images.
B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
C. Use a function with an external image management library. Associate the function with the CloudFront behaviors that serve the images.
D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Answer: C

Explanation:

- A: High operational burden, EC2 scaling needed.

- B: Origin request policies don't transform content.

- C: Correct, runs at edge with custom logic for resizing.

- D: Response headers policy cannot resize images.

Question: 959

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

Options:

A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.

B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.

C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.

D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

Answer: C

Explanation:

- A: ACM certs don't enforce PHI compliance directly.

- B: SSE-S3 keys are AWS-managed, not administered by the compliance team.

- C: Correct, SSE-KMS + aws:SecureTransport satisfies in-transit + at-rest encryption with customer key management.

- D: Macie helps with PII discovery, not encryption management.

Question: 960

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code?

Options:

A. Add an X-API-Key header in the HTTP header for authorization.

B. Use an interface endpoint.

C. Use a gateway endpoint.

D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

Answer: B

Explanation:

- A: API key headers don't fix routing path.

- B: Correct, interface VPC endpoint ensures API Gateway private APIs communicate within VPC.

- C: Gateway endpoints are only for S3/DynamoDB.

- D: SQS adds overhead, not required.

Question: 961

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.
Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.

B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.

C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.

D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

Answer: C

Explanation:

- A: RDS adds operational overhead.

- B: S3 + Athena works, but no sub-ms latency.

- C: Correct, DynamoDB+DAX = sub-ms reads, Athena for ad-hoc queries on exported data.

- D: Adds unnecessary Kinesis complexity.

Question: 962
A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.
Which actions should a solutions architect take to meet this requirement? (Choose two.)

Options:
A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer: BE

Explanation:

- A: DynamoDB doesn't guarantee ordered message delivery.

- B: Correct, Kinesis shards guarantee ordering per partition key.

- C: Memcached not meant for ordered message delivery.

- D: Standard SQS doesn't guarantee ordering.

- E: Correct, SQS FIFO queues guarantee order within message group ID.

Question: 963
A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.
Which solution will meet these requirements?

Options:
A. Amazon EventBridge event bus
B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
C. Amazon Simple Notification Service (Amazon SNS) standard topics
D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Answer: B

Explanation:

- A: EventBridge doesn't guarantee order.

- B: Correct, SNS FIFO topics guarantee ordered delivery and fan-out.

- C: Standard SNS has no ordering guarantee.

- D: SQS FIFO queues keep order but don't fan out to multiple services.

Question: 964

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data.

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

Options:

A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.

B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.

C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.

D. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

Answer: BD

Explanation:

- A: Only partially secures SQS, no KMS fine-grained control.

- B: Correct, SSE-KMS for SNS with restricted key policy.

- C: Does not cover all encryption needs.

- D: Correct, SSE-KMS for SQS with TLS condition ensures security.

- E: IAM policy not enough, KMS policy is required.

Question: 965

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

Options:

A. Read replicas
B. Manual snapshots
C. Automated backups
D. Multi-AZ deployments

Answer: C

Explanation:

- A: Read replicas help with scaling, not PITR.

- B: Manual snapshots don't allow 5-min recovery.

- C: Correct, automated backups enable point-in-time recovery.

- D: Multi-AZ ensures HA, not recovery to past state.

Question: 966

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

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

Options:

A. Enable API caching and throttling on the API Gateway API.
B. Set up AWS WAF on the API Gateway API. Create a rule to filter users who have a subscription.
C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

Answer: D

Explanation:

- A: Caching doesn't enforce access control.

- B: WAF filters requests, not subscription checks.

- C: DynamoDB IAM fine-grained access is complex here.

- D: Correct, API Gateway usage plans and API keys enforce subscription-based access.

Question: 967

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

Options:

A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.

B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.

C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Answer: A

Explanation:

- A: Correct, Global Accelerator with NLB improves latency + availability for UDP apps.

- B: ALB doesn't support UDP.

- C: CloudFront doesn't support UDP.

- D: Same issue as above, ALB+CloudFront won't work for UDP.

Question: 968

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords.
What should the solutions architect do to accomplish this?

Options:

A. Set an overall password policy for the entire AWS account.
B. Set a password policy for each IAM user in the AWS account.
C. Use third-party vendor software to set password requirements.
D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Answer: A

Explanation:

- A: Correct, account-wide IAM password policy enforces complexity + rotation.

- B: Per-user policy is not possible.

- C: Third-party tools unnecessary.

- D: CloudWatch cannot enforce password rules.

Question: 969

A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.
Which solution will meet these requirements with the LEAST operational overhead?

Options:

A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Answer: A

Explanation:

- A: Correct, AWS Batch handles multi-language scheduled jobs with scaling.

- B: App Runner not designed for scheduled tasks.

- C: Lambda runtime limits (15 min max) unsuitable for 1-hour tasks.

- D: ASG of AMIs doesn't reduce operational complexity.

Question: 970
A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.
Which solution meets these requirements?

Options:
A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

Answer: C

Explanation:

- A: NAT instance requires management overhead.

- B: NAT instance in private subnet won't provide internet access.

- C: Correct, NAT gateway in public subnet is managed and scalable.

- D: NAT gateway in private subnet won't work.

Question: 971
A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).
Which combination of actions will meet this requirement with the LEAST operational overhead? (Choose two.)

Options:
A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Answer: C, D

Explanation:

- A: Plugins add unnecessary complexity.

- B: Manual per-volume encryption adds overhead.

- C: Correct, EBS default encryption with customer key ensures all volumes encrypted.

- D: Correct, IAM role allows EKS to use customer-managed KMS key.

- E: Not secure and not supported best practice.

Question: 972
A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.
When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.
Which solution meets these requirements MOST cost-effectively?

Options:
A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
D. Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.

Answer: D

Explanation:

- A: Storing large images in RDS is costly and inefficient.

- B: DynamoDB not optimized for large object storage.

- C: Same issue, DynamoDB not for images.

- D: Correct, S3 for image storage + DB for metadata = scalable and cost-effective.

Question: 973
A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models. Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.
Which storage solution meets these requirements MOST cost-effectively?

Options:
A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer: D

Explanation:

- A: Intelligent-Tiering has monitoring cost; trillions of objects = expensive.

- B: Same issue as A.

- C: Standard-IA only after 30 days doesn't cover frequent early access.

- D: Correct, S3 Standard first, then IA after 30 days, Glacier Deep Archive after 1 year.

Question: 974
A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.
A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.
Which solution meets these requirements?

Options:
A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Answer: D

Explanation:

- A: VPN not ideal for large consistent data transfers.

- B: Adds unnecessary cost and complexity.

- C: Three separate Direct Connects are costly.

- D: Correct, one DX + transit gateway handles all VPCs and on-premises efficiently.

Question: 975

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.

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

Options:

A. Use AWS Step Functions to build the application.
B. Integrate all the application components in an AWS Glue job.
C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
D. Use AWS Lambda functions and Amazon EventBridge events to build the application.

Answer: A

Explanation:

- A: Correct, Step Functions orchestrates Lambda, EC2, on-prem tasks with minimal ops.

- B: Glue is for ETL, not workflow orchestration.

- C: SQS provides queuing but not orchestration.

- D: EventBridge alone doesn't handle orchestration/approvals.

Question: 976

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

Options:

A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
B. Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.
C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
D. Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

Answer: A

Explanation:

- A: Correct, RDS Proxy manages and pools connections for serverless workloads.

- B: Caching doesn't solve DB connection limits.

- C: Bigger instance won't fix spiky connections.

- D: Multi-AZ is for HA, not connection handling.

Question: 977

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

Options:

A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.

B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.

C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.

D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

Answer: B

Explanation:

- A: Lambda polling adds delay and overhead.

- B: Correct, lifecycle hooks directly tie to launch/terminate events.

- C: User data only runs at launch, not termination.

- D: No direct hook for termination, unreliable.

Question: 978

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

Options:

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.

B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.

C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.

D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Answer: B

Explanation:

- A: Aurora not ideal for massive scaling of game events.

- B: Correct, NLB supports UDP + DynamoDB on-demand scales automatically.

- C: Aurora Global Database adds unnecessary cost and latency.

- D: ALB doesn't support UDP.

Question: 979

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.

Which solution will meet these requirements?

Options:

A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.

B. Configure provisioned concurrency for the Lambda function that handles the requests.

C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.

D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

Answer: B

Explanation:

- A: Bypassing API Gateway removes abstraction and auth.

- B: Correct, provisioned concurrency keeps Lambdas warm, lowering cold start latency.

- C: Caching in S3 is not efficient for dynamic queries.

- D: Bigger DB doesn't fix Lambda cold starts.

Question: 980

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirements?

Options:

A. Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.

B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.

C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.

D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

Answer: D

Explanation:

- A: RDS cannot scale to zero.

- B: Marketplace adds cost and complexity.

- C: Running an extra EC2 for scheduling increases overhead.

- D: Correct, EventBridge + Lambda is serverless, automated, low ops.

Question: 981

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently.

The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.

Which solution will meet these requirements with the LEAST amount of change to the application code?

Options:

A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.

B. Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.

C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.

D. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

Answer: B

Explanation:

- A: DocumentDB not required; relational queries already work.

- B: Correct, Aurora Replica allows offloading reporting without affecting primary.

- C: Multi-AZ standby cannot serve reads.

- D: DynamoDB requires major app code changes.

Question: 982

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

Options:

A. Configure a TLS listener. Deploy the server certificate on the NLB.

B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.

C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.

D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

Answer: A

Explanation:

- A: Correct, TLS listener on NLB encrypts data in transit.

- B: Protects from DDoS, not in-transit encryption.

- C: ALB supports TLS but NLB + TLS is simpler here.

- D: EBS encryption is at rest, not in transit.

Question: 983

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

Options:
A. Dedicated Reserved Hosts
B. Dedicated On-Demand Hosts
C. Dedicated Reserved Instances
D. Dedicated On-Demand Instances

Answer: A

Explanation:

- A: Correct, Reserved Hosts allow BYOL with license compliance + lowest cost.

- B: On-Demand Hosts are costly for predictable use.

- C: Reserved Instances don't provide socket/core control.

- D: On-Demand Instances costly, no license mapping.

Question: 984

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time.

Which solution will meet these requirements MOST cost-effectively?

Options:
A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

Answer: C

Explanation:

- A: S3 is not POSIX-compliant.

- B: Same as A.

- C: Correct, EFS is POSIX-compliant, highly available, and lifecycle to IA saves cost.

- D: One Zone EFS lacks multi-AZ HA.

Question: 985

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

Options:

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Answer: C

Explanation:

- A: Too open; web servers don't need 0.0.0.0/0 access.

- B: NACLs are stateless; SGs are better for fine control.

- C: Correct, SG from LB to web, web to DB = least privilege.

- D: Using NACL instead of SG adds complexity.

Question: 986

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

Options:

A. Implement Amazon SNS to store the database calls.
B. Implement Amazon ElastiCache to cache the large datasets.
C. Implement an RDS for MySQL read replica to cache database calls.
D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

Explanation:

- A: SNS is for messaging, not caching.

- B: Correct, ElastiCache reduces repeated DB queries by caching results.

- C: Read replicas help scale reads but not cache repeated queries efficiently.

- D: Firehose streams data, not for query acceleration.

Question: 987

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

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

Options:

A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.

B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.

C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.

D. Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.

E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

Answer: D, E

Explanation:

- A: Root user should never be used.

- B: PowerUsers give broader permissions than required.

- C: Admin policy violates least privilege.

- D: Correct, restrict IAM policy to CloudFormation only.

- E: Correct, IAM role with explicit CloudFormation permissions ensures security.

Question: 988

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

Options:

A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.

B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.

C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.

D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tiers security group.

Answer: D

Explanation:

- A: Default NACLs already allow traffic.

- B: Default route tables already allow VPC internal communication.

- C: They're in same VPC, so peering unnecessary.

- D: Correct, SG must allow web SG to connect on port 3306.

Question: 989

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

Options:

A. Deploy RDS read replicas to process the business reporting queries.

B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.

C. Scale up the DB instance to a larger instance type to handle write operations and queries.

D. Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

Answer: A

Explanation:

- A: Correct, read replicas offload queries.

- B: RDS cannot scale horizontally like ELB.

- C: Bigger instance doesn't separate reads from writes.

- D: Multi-AZ provides HA, not read offloading.

Question: 990

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

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

Options:

A. Turn on the sticky sessions feature (session affinity) on the ALB.

B. Use an Amazon DynamoDB table to store customer session information.

C. Deploy an Amazon Cognito user pool to manage user session information.

D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.

E. Use AWS Systems Manager Application Manager in the application to manage user session information.

Answer: A, D

Explanation:

- A: Sticky sessions help tie users to instances.

- B: DynamoDB not ideal for short-lived session data.

- C: Cognito is for identity, not session store.

- D: Correct, Redis is fast, durable session store.

- E: Systems Manager not relevant.

Question: 991

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours. The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?

Options:

A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.

B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.

C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

Answer: C

Explanation:

- A: EBS snapshots of ephemeral stateless EC2 unnecessary.

- B: AMIs missing, only covers EBS.

- C: Correct, stateless tiers use AMIs, DB uses automated PITR backups.

- D: Same issue, EBS snapshots of stateless don't matter.

Question: 992

A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.

The application must be secure and accessible for global customers that have dynamic IP addresses.

How should a solutions architect configure the security groups to meet these requirements?

Options:

A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.

B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.

C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.

D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

Answer: A

Explanation:

- A: Correct, secure DB to only web SG, web open to HTTPS globally.

- B: Dynamic customer IPs make allow-listing impractical.

- C: Same issue as B, insecure for DB.

- D: Opening DB to world is insecure.

Question: 993

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.

What should a solutions architect do to meet these requirements?

Options:

A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.

B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.

C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.

D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.

Answer: C

Explanation:

- A: Kinesis Video Streams not needed.

- B: Textract extracts from documents, not audio.

- C: Correct, Transcribe + PII redaction fits perfectly.

- D: Amazon Connect is for live calls, not post-processing.

Question: 994
A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.
A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.
What should a solutions architect do to improve the application performance?

Options:
A. Replace the volume with a magnetic volume.
B. Increase the number of IOPS on the gp3 volume.
C. Replace the volume with a Provisioned IOPS SSD (io2) volume.
D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

Answer: D

Explanation:

- A: Magnetic volumes are slower.

- B: gp3 IOPS max still limited.

- C: io2 costlier and unnecessary if gp3 parallelization works.

- D: Correct, splitting into multiple gp3 volumes increases aggregate throughput.

Question: 995
An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.
Which service should the solutions architect use to find the desired information?

Options:
A. Amazon GuardDuty
B. Amazon Inspector
C. AWS CloudTrail
D. AWS Config

Answer: C

Explanation:

- A: GuardDuty detects threats, not change history.

- B: Inspector scans for vulnerabilities.

- C: Correct, CloudTrail records API calls by IAM users.

- D: Config tracks configuration but not who made changes.

Question: 996
A company has implemented a self-managed DNS service on AWS. The solution consists of the following:
• Amazon EC2 instances in different AWS Regions
• Endpoints of a standard accelerator in AWS Global Accelerator
The company wants to protect the solution against DDoS attacks.
What should a solutions architect do to meet this requirement?

Options:
A. Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.
B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.
C. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.
D. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.

Answer: A

Explanation:

- A: Correct, Shield Advanced protects Global Accelerator endpoints from DDoS.

- B: EC2 instances not directly protected via Shield.

- C: WAF doesn't protect against large-scale DDoS.

- D: Same issue as C.

Question: 997
An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.
A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.
Which solution meets these requirements?

Options:
A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

Answer: C

Explanation:

- A: Lambda max size and timeout unsuitable for 10GB/1h jobs.

- B: Same as A.

- C: Correct, ECS Fargate runs container jobs with no infra management.

- D: EC2 launch type adds ops overhead.

Question: 998
A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.
Which solution meets these requirements MOST cost-effectively?

Options:
A. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.
B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

Answer: C

Explanation:

- A: 600 TB over 100 Mbps takes months, not 2 weeks.

- B: Same bottleneck as A.

- C: Correct, Snowball Edge transfers PB-scale data securely and quickly.

- D: DX setup takes months, not feasible in 2 weeks.

Question: 999
A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.
A solutions architect must design a solution to protect the application from this type of attack.
Which solution meets these requirements with the LEAST operational overhead?

Options:

A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.

B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.

C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.

D. Create an Amazon CloudFront distribution with in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Answer: B

Explanation:

- A: CloudFront helps caching but not rate-limiting.

- B: Correct, WAF rate-based rule blocks HTTP flood.

- C: Alerts only, no automatic protection.

- D: Lambda@Edge adds overhead.

Question: 1000

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

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

Options:

A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.

B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.

C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.

D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Answer: C

Explanation:

- A: Transactions don't send notifications.

- B: Requires app modification, higher overhead.

- C: Correct, Streams + SNS integration is serverless and minimal ops.

- D: Cron scanning adds delay and overhead.