

1. 英文 SAA-C03 考试认证题库

[单选题]

1. Question #1A 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?
- 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.

答案：A

解析：S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets, especially for large data volumes and high-speed internet connections. It leverages the AWS global network and accelerates the transfer of large files from remote locations by using edge locations. This service requires minimal changes to the existing infrastructure and does not add significant operational complexity, making it the most suitable option for quickly aggregating

data into a single S3 bucket with high-speed internet connections at each site.

解析: S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets, especially for large data volumes and high-speed internet connections. It leverages the AWS global network and accelerates the transfer of large files from remote locations by using edge locations. This service requires minimal changes to the existing infrastructure and does not add significant operational complexity, making it the most suitable option for quickly aggregating data into a single S3 bucket with high-speed internet connections at each site.

2. Question #2A 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?

- 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.

答案: C

解析: Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon S3 using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds. This approach allows for on-demand querying without the need to move data or set up additional infrastructure, thus minimizing operational overhead and changes to the existing architecture.

解析: Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon S3 using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds. This approach allows for on-demand querying without the need to move data or set up additional infrastructure, thus minimizing operational overhead and changes to the existing architecture.

3. Question #3A 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?

- 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.

答案: A

解析: By adding the aws:PrincipalOrgID global condition key to the S3 bucket policy with a reference to the organization ID, you can restrict access to the bucket to only users of accounts within the specified organization. This approach is straightforward and does not require ongoing management or monitoring of events, tagging of users, or creation of organizational units. It leverages the existing AWS Organizations structure to manage access control, thereby reducing operational overhead.

解析: By adding the aws:PrincipalOrgID global condition key to the S3 bucket policy with a reference to the organization ID, you can restrict access to the bucket to only users of accounts within the specified organization. This approach is straightforward and does not require ongoing management or monitoring of events, tagging of users, or creation of organizational units. It leverages the existing AWS Organizations structure to manage access control, thereby reducing operational overhead.

4. Question #4An 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?
- 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.

答案: A

解析: A gateway VPC endpoint to the S3 bucket allows the EC2 instance to access the S3 bucket over AWS's private network, without the need for internet connectivity. VPC endpoints provide private connectivity to AWS services, ensuring that traffic stays within the AWS network and does not traverse the public internet, thus enhancing security and potentially reducing latency.

解析: A gateway VPC endpoint to the S3 bucket allows the EC2 instance to access the S3 bucket over AWS's private network, without the need for internet connectivity. VPC endpoints provide private connectivity to AWS services, ensuring that traffic stays within the AWS network and does not traverse the public internet, thus enhancing security and potentially reducing latency.

5. Question #5A 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?

- 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.

答案: C

解析: By copying the data from both EBS volumes to Amazon EFS and modifying the application to save new documents to EFS, you create a centralized and scalable file storage system that can be accessed by both EC2 instances. Amazon EFS is designed to provide a shared file system that can be mounted by multiple instances, ensuring that all documents are available to users regardless of which instance serves their request. This approach enhances scalability and availability, as EFS can easily handle concurrent access and growth in the number of documents.

解析: By copying the data from both EBS volumes to Amazon EFS and modifying the application to save new documents to EFS, you create a centralized and scalable file storage system that can be accessed by both EC2 instances. Amazon EFS is designed to provide a shared file system that can be mounted by multiple instances, ensuring that all documents are available to users regardless of which instance serves their request. This approach enhances scalability and availability, as EFS can easily handle concurrent access and growth in the number of documents.

6. Question #7A 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?

- 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.

答案：D

解析：Using Amazon SNS and SQS allows for the decoupling of the message ingestion and consumption processes. SNS can handle high throughputs and sudden spikes in message volume, and SQS provides a scalable and reliable queuing mechanism for processing messages. This approach enables the system to scale horizontally as needed, handling the varying load and ensuring that all messages are processed.

解析：Using Amazon SNS and SQS allows for the decoupling of the message ingestion and consumption processes. SNS can handle high throughputs and sudden spikes in message volume, and SQS provides a scalable and reliable queuing mechanism for processing messages. This approach enables the system to scale horizontally as needed, handling the varying load and ensuring that all messages are processed.

7. Question #8A 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?

- 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.

答案: B

解析: Configuring Amazon SQS as a job queue and using EC2 Auto Scaling based on the size of the queue allows for the system to automatically adjust the number of compute nodes based on the workload. This approach provides both resiliency and scalability, as it can handle variable workloads and ensure that jobs are processed efficiently without overprovisioning resources.

解析: Configuring Amazon SQS as a job queue and using EC2 Auto Scaling based on the size of the queue allows for the system to automatically adjust the number of compute nodes based on the workload. This approach provides both resiliency and scalability, as it can handle variable workloads and ensure that jobs are processed efficiently without

overprovisioning resources.

8. Question #9A 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?

- 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.

答案：B

解析：Amazon S3 File Gateway allows for the extension of storage capacity while maintaining low-latency access to recently accessed files through local caching. The S3 Lifecycle policy can be used to automatically transition files to S3 Glacier Deep Archive after 7 days, providing a cost-effective storage solution for infrequently accessed data. This approach manages the file lifecycle effectively and prevents storage capacity issues in the future.

解析：Amazon S3 File Gateway allows for the extension of storage capacity while maintaining low-latency access to recently accessed files through local caching. The S3 Lifecycle policy can be used to automatically transition files to S3 Glacier Deep Archive after 7 days, providing a cost-effective storage solution for infrequently accessed data. This

approach manages the file lifecycle effectively and prevents storage capacity issues in the future.

9. Question #10A 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?

- 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.

答案: B

解析: Based on the company's requirement to ensure that orders are processed in the order they are received for their ecommerce web application, the best solution is: 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. This solution is the most appropriate because: 1. FIFO (First-In-First-Out) queues: SQS FIFO queues guarantee that messages are processed in the exact order they are sent, which aligns with the requirement to process orders in the order they are received. 2. Decoupling: Using SQS between API Gateway and Lambda provides a buffer, allowing the system to handle high volumes of incoming

orders without overwhelming the processing function.

3. Scalability: This architecture can easily scale to handle varying loads of incoming orders.

4. Reliability: If the Lambda function fails to process an order, the message remains in the queue and can be retried, ensuring no orders are lost.

5. Integration simplicity: API Gateway can easily integrate with SQS, and SQS can trigger Lambda functions for processing. To implement this solution:

1. Create an SQS FIFO queue.
2. Set up an API Gateway REST API with an integration to send messages to the SQS FIFO queue.
3. Configure the SQS FIFO queue to trigger a Lambda function for order processing.
4. Implement the order processing logic in the Lambda function.

Best practices to consider:

- Implement proper error handling and dead-letter queues to manage failed processing attempts.
- Use appropriate IAM roles and policies to ensure secure access between services.
- Monitor the queue length and Lambda function performance to optimize processing capacity.
- Implement idempotency in your Lambda function to handle potential duplicate messages.

Remember to test this setup thoroughly in a non-production environment before deploying to production. For the most up-to-date information on service limits and best practices, always refer to the official AWS documentation.

Sources

[1] [API Gateway REST APIs – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-rest-api.html>) [3]

[Amazon API Gateway – AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda] (<https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/amazon-api-gateway.html>) [6]

[Welcome – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/api/Welcome.html>)

解析: Based on the company's requirement to ensure that orders are processed in the order they are received for their ecommerce web application, the best solution is:

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. This solution is the most appropriate because:

1. FIFO (First-In-First-Out) queues: SQS FIFO queues guarantee that messages are processed in the exact order they are sent,

which aligns with the requirement to process orders in the order they are received.

2. Decoupling: Using SQS between API Gateway and Lambda provides a buffer, allowing the system to handle high volumes of incoming orders without overwhelming the processing function.

3. Scalability: This architecture can easily scale to handle varying loads of incoming orders.

4. Reliability: If the Lambda function fails to process an order, the message remains in the queue and can be retried, ensuring no orders are lost.

5. Integration simplicity: API Gateway can easily integrate with SQS, and SQS can trigger Lambda functions for processing.

To implement this solution:

1. Create an SQS FIFO queue.
2. Set up an API Gateway REST API with an integration to send messages to the SQS FIFO queue.
3. Configure the SQS FIFO queue to trigger a Lambda function for order processing.
4. Implement the order processing logic in the Lambda function.

Best practices to consider:

- Implement proper error handling and dead-letter queues to manage failed processing attempts.
- Use appropriate IAM roles and policies to ensure secure access between services.
- Monitor the queue length and Lambda function performance to optimize processing capacity.
- Implement idempotency in your Lambda function to handle potential duplicate messages.

Remember to test this setup thoroughly in a non-production environment before deploying to production. For the most up-to-date information on service limits and best practices, always refer to the official AWS documentation.

Sources

- [1] [API Gateway REST APIs – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-rest-api.html>) [3]
- [Amazon API Gateway – AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda] (<https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/amazon-api-gateway.html>) [6]
- [Welcome – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/api>Welcome.html>)

10. Question #11A 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 user names 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?

- 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 that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.
- D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance.
Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

答案：A

解析：AWS Secrets Manager is designed to manage secrets like database credentials, API keys, and other sensitive information. By enabling automatic rotation, the solution not only centralizes the management of credentials but also ensures that they are regularly rotated, enhancing security and reducing the operational overhead of manual credential management.

解析：AWS Secrets Manager is designed to manage secrets like database credentials, API keys, and other sensitive information. By enabling automatic rotation, the solution not only centralizes the management of credentials but also ensures that they are regularly rotated, enhancing security and reducing the operational overhead of manual credential management.

11. Question #12 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?

- 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. Create a custom domain name that points to the accelerator DNS name. Use the custom domain name as an endpoint for the web application.
- 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. Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content. Point the other domain name to the accelerator DNS name for static content. Use the domain names as endpoints for the web application.

答案：A

解析：By creating an Amazon CloudFront distribution with both the S3 bucket and the ALB as origins, the company can effectively cache the static and dynamic content closer to the users, thereby reducing latency and improving performance. Configuring Route 53 to route traffic to the CloudFront distribution ensures that the content is efficiently delivered to the end-users, regardless of their location.

解析：By creating an Amazon CloudFront distribution with both the S3 bucket and the ALB as origins, the company can effectively cache the static and dynamic content closer to the users, thereby reducing latency and improving performance. Configuring Route 53 to route traffic to the CloudFront distribution ensures that the content is efficiently delivered to the end-users, regardless of their location.

12. Question #13A 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?

- A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.
- B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter. Use multi-Region secret replication for the required Regions. Configure Systems Manager to rotate the secrets on a schedule.
- C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.
- D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys. Store the secrets in an Amazon DynamoDB global table. Use an AWS Lambda function to retrieve the secrets from DynamoDB. Use the RDS API to rotate the secrets.

答案: A

解析: AWS Secrets Manager is specifically designed for managing and rotating secrets, including database credentials, across multiple regions. By using multi-Region secret replication and scheduling the rotation, the solution minimizes operational overhead by automating the credential rotation process and ensuring that credentials are securely managed.

解析: AWS Secrets Manager is specifically designed for managing and rotating secrets, including database credentials, across multiple regions. By using multi-Region secret replication and scheduling the rotation, the solution minimizes operational overhead by automating the credential rotation process and ensuring that credentials are securely managed.

13. Question #14 A company runs an ecommerce application 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 based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is

hosted on a large EC2 instance. The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability. Which solution will meet these requirements?

- A. Use Amazon Redshift with a single node for leader and compute functionality.
- B. Use Amazon RDS with a Single-AZ deployment. Configure Amazon RDS to add reader instances in a different Availability Zone.
- C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

答案：C

解析：Amazon Aurora is a MySQL-compatible relational database that provides high performance and high availability. A Multi-AZ deployment of Aurora automatically maintains a synchronous standby replica in a different Availability Zone, ensuring high availability. Configuring Aurora Auto Scaling with Aurora Replicas allows the database to automatically scale out by adding more read replicas in response to increased read workloads, thus meeting the demand of unpredictable read workloads while maintaining high availability.

解析：Amazon Aurora is a MySQL-compatible relational database that provides high performance and high availability. A Multi-AZ deployment of Aurora automatically maintains a synchronous standby replica in a different Availability Zone, ensuring high availability. Configuring Aurora Auto Scaling with Aurora Replicas allows the database to automatically scale out by adding more read replicas in response to increased read workloads, thus meeting the demand of unpredictable read workloads while maintaining high availability.

14. Question #15A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center.

The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud. Which solution will meet these requirements?

- A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.
- B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
- C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.
- D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

答案: C

解析: AWS Network Firewall is a stateful, managed network firewall service designed for protecting traffic flowing in and out of a VPC. It allows the creation of rules for traffic inspection and filtering, providing the same functionalities that the on-premises inspection server offered. This solution meets the company's requirements by protecting the VPC traffic with minimal operational overhead.

解析: AWS Network Firewall is a stateful, managed network firewall service designed for protecting traffic flowing in and out of a VPC. It allows the creation of rules for traffic inspection and filtering, providing the same functionalities that the on-premises inspection server offered. This solution meets the company's requirements by protecting the VPC traffic with minimal operational overhead.

15. Question #16 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 data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access. Which solution will meet these requirements?

- A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.
- B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.
- C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
- D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

答案：B

解析：Amazon QuickSight is a business intelligence service that can connect to multiple data sources, including Amazon S3 and Amazon RDS for PostgreSQL, and create interactive visualizations. By publishing dashboards and sharing them with specific users and groups, the company can control access to the visualizations, granting full access to the management team and limited access to the rest of the company. This solution meets the requirements for data visualization and access control.

解析：Amazon QuickSight is a business intelligence service that can connect to multiple data sources, including Amazon S3 and Amazon RDS for PostgreSQL, and create interactive visualizations. By publishing dashboards and sharing them with specific users and groups, the company can control access to the visualizations, granting full access to the management team and limited access to the rest of the company. This solution meets the requirements for data visualization and access control.

16. Question #17 A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3

bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket. What should the solutions architect do to meet this requirement?

- A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
- B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.
- C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
- D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

答案：A

解析：IAM roles are AWS identities that can be assigned permissions to access AWS resources. By creating an IAM role with the necessary permissions for the S3 bucket and attaching it to the EC2 instances, the instances will be able to access the bucket and the documents stored within it. This is the recommended approach for granting access to AWS resources from EC2 instances.

解析：IAM roles are AWS identities that can be assigned permissions to access AWS resources. By creating an IAM role with the necessary permissions for the S3 bucket and attaching it to the EC2 instances, the instances will be able to access the bucket and the documents stored within it. This is the recommended approach for granting access to AWS resources from EC2 instances.

17. Question #19A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets. A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server. Which solution will meet these requirements with

the LEAST operational overhead?

- A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- C. Deploy a transit gateway in the inspection VPC. Configure route tables to route the incoming packets through the transit gateway.
- D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

答案: D

解析: Deploying a Gateway Load Balancer in the inspection VPC and creating a Gateway Load Balancer endpoint to receive and forward incoming packets to the virtual firewall appliance is the most efficient solution. Gateway Load Balancer operates at the network layer (Layer 3) and is designed to handle high-performance network traffic, making it suitable for inspecting traffic before it reaches the web servers. This solution requires minimal configuration changes and leverages the managed nature of the Gateway Load Balancer, resulting in the least operational overhead.

解析: Deploying a Gateway Load Balancer in the inspection VPC and creating a Gateway Load Balancer endpoint to receive and forward incoming packets to the virtual firewall appliance is the most efficient solution. Gateway Load Balancer operates at the network layer (Layer 3) and is designed to handle high-performance network traffic, making it suitable for inspecting traffic before it reaches the web servers. This solution requires minimal configuration changes and leverages the managed nature of the Gateway Load Balancer, resulting in the least operational overhead.

18. Question #20 A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS

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

- A. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.
- B. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.
- C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
- D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

答案：D

解析：Using the EBS fast snapshot restore feature minimizes the time required to clone data into a test environment. This feature allows for the rapid restoration of EBS snapshots into new EBS volumes, which can then be attached to EC2 instances in the test environment. The restored volumes will have their data fully initialized and ready for access, providing the high I/O performance required by the software.

解析：Using the EBS fast snapshot restore feature minimizes the time required to clone data into a test environment. This feature allows for the rapid restoration of EBS snapshots into new EBS volumes, which can then be attached to EC2 instances in the test environment. The restored volumes will have their data fully initialized and ready for access, providing the high I/O performance required by the software.

19. Question #21 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?

- 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.

答案：D

解析：The combination of using Amazon S3 for hosting static content, Amazon CloudFront for content distribution, and AWS Lambda with Amazon API Gateway for backend processing provides a highly scalable and low-latency solution. Storing data in Amazon DynamoDB ensures high-performance access, even at peak loads. This serverless architecture minimizes operational overhead and allows the website to handle millions of requests with the required millisecond latency.

解析：The combination of using Amazon S3 for hosting static content, Amazon CloudFront for content distribution, and AWS Lambda with Amazon API Gateway for backend processing provides a highly scalable and low-latency solution. Storing data in Amazon DynamoDB ensures high-performance access, even at peak loads. This serverless architecture

minimizes operational overhead and allows the website to handle millions of requests with the required millisecond latency.

20. Question #22A 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?

- 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)

答案：B

解析：S3 Intelligent-Tiering automatically moves data to the most cost-effective storage tier based on access patterns, making it suitable for media files with unpredictable access patterns. It stores objects in two access tiers: frequent access and infrequent access. This feature ensures that frequently accessed files are stored at a lower cost while still providing high availability and resilience against the loss of an Availability Zone.

解析：S3 Intelligent-Tiering automatically moves data to the most cost-effective storage tier based on access patterns, making it suitable for media files with unpredictable access patterns. It stores objects in two access tiers: frequent access and infrequent access. This feature ensures that frequently accessed files are stored at a lower cost while still providing high availability and resilience against the loss of an Availability Zone.

21. Question #23 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?

- 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.

答案：B

解析：S3 Glacier Deep Archive is the lowest-cost storage class in Amazon S3, making it the most cost-effective solution for storing infrequently accessed data that is not expected to be retrieved for an extended period. By creating an S3 Lifecycle configuration to transition the backup files to S3 Glacier Deep Archive after 1 month, the company can ensure long-term storage at the lowest possible cost.

解析：S3 Glacier Deep Archive is the lowest-cost storage class in Amazon S3, making it the most cost-effective solution for storing infrequently accessed data that is not expected to be retrieved for an extended period. By creating an S3 Lifecycle configuration to transition the backup files to S3 Glacier Deep Archive after 1 month, the company can ensure long-term storage at the lowest possible cost.

22. Question #24 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?

- 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.

答案：B

解析：AWS Cost Explorer provides a detailed view of cost and usage data over time, allowing users to analyze and identify trends and anomalies. By using Cost Explorer's granular filtering feature, the architect can focus on EC2 costs and instance types to pinpoint the cause of the vertical scaling, all without the need for additional tools or complex report generation processes.

解析：AWS Cost Explorer provides a detailed view of cost and usage data over time, allowing users to analyze and identify trends and anomalies. By using Cost Explorer's granular filtering feature, the architect can focus on EC2 costs and instance types to pinpoint the cause of the vertical scaling, all without the need for additional tools or complex report generation processes.

23. Question #25A 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?

- 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.

答案：D

解析：By decoupling the Lambda functions using an Amazon SQS queue, the solution improves scalability and reduces configuration effort. The first Lambda function can receive information and then place the information onto the SQS queue. The second Lambda function can process the queue at a pace that is optimized for database operations, thus avoiding the bottleneck caused by direct invocation, which is the case with Amazon SNS in option C.

解析：By decoupling the Lambda functions using an Amazon SQS queue, the solution improves scalability and reduces configuration effort. The first Lambda function can receive information and then place the information onto the SQS queue. The second Lambda function can process the queue at a pace that is optimized for database operations, thus avoiding the bottleneck caused by direct invocation, which is the case with Amazon SNS in option C.

24. Question #26A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes. What should a solutions architect do to accomplish this goal?

- 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).

答案：A

解析: AWS Config is designed to monitor and record changes to the configuration of AWS resources, including S3 buckets. By turning on AWS Config and setting up appropriate rules, the architect can track changes to the S3 buckets and receive notifications if any unauthorized changes occur.

解析: AWS Config is designed to monitor and record changes to the configuration of AWS resources, including S3 buckets. By turning on AWS Config and setting up appropriate rules, the architect can track changes to the S3 buckets and receive notifications if any unauthorized changes occur.

25. Question #27A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege. Which solution will meet these requirements?

- A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
- B. Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.
- C. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
- D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

答案：A

解析：Sharing the CloudWatch dashboard with the product manager via email allows them to access the dashboard without needing an AWS account or IAM user. This approach follows the principle of least privilege by granting the product manager access only to the specific dashboard, without providing broader access to AWS resources.

解析：Sharing the CloudWatch dashboard with the product manager via email allows them to access the dashboard without needing an AWS account or IAM user. This approach follows the principle of least privilege by granting the product manager access only to the specific dashboard, without providing broader access to AWS resources.

26. Question #28A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory. Which solution will meet these requirements?

- A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
- D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

答案：B

解析：To enable SSO across all AWS accounts managed by AWS Organizations and to continue managing users and groups in the on-premises Active

Directory, a two-way forest trust is required. This trust relationship allows for authentication and authorization between the on-premises Active Directory and AWS SSO, enabling seamless access to AWS resources while maintaining control over user identities.

解析: To enable SSO across all AWS accounts managed by AWS Organizations and to continue managing users and groups in the on-premises Active Directory, a two-way forest trust is required. This trust relationship allows for authentication and authorization between the on-premises Active Directory and AWS SSO, enabling seamless access to AWS resources while maintaining control over user identities.

27. Question #29A 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?

- 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.

答案: A

解析: AWS Global Accelerator is designed to improve the performance of applications that use UDP connections by routing user traffic to the optimal AWS Region based on latency. By deploying an NLB in each Region and using it as an endpoint for Global Accelerator, the company can ensure that users are routed to the Region with the lowest latency, and the Auto Scaling group can handle automated failover between Regions if an instance or a Region becomes unavailable.

解析: AWS Global Accelerator is designed to improve the performance of applications that use UDP connections by routing user traffic to the optimal AWS Region based on latency. By deploying an NLB in each Region and using it as an endpoint for Global Accelerator, the company can ensure that users are routed to the Region with the lowest latency, and the Auto Scaling group can handle automated failover between Regions if an instance or a Region becomes unavailable.

28. Question #30A 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?

- 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.

答案: A

解析: To address the development team's requirement of reducing costs for their monthly resource-intensive tests on the Amazon RDS for MySQL DB instance without reducing compute and memory attributes, the most

cost-effective solution is:

- A. Stop the DB instance when tests are completed. Restart the DB instance when required. This approach offers several benefits:
 - 1. Cost Savings: When you stop an RDS instance, you only pay for the storage and any associated backups. You're not charged for the compute capacity while the instance is stopped, which can lead to significant cost savings, especially for a DB instance that's only used for 48 hours each month.
 - 2. Maintains Instance Attributes: Stopping and starting the instance preserves all the compute and memory attributes, meeting the requirement not to reduce these resources.
 - 3. Quick Availability: Restarting a stopped RDS instance is typically faster than creating a new instance from a snapshot, making the database available quickly when needed for the next testing cycle.
 - 4. Simplicity: This solution is straightforward to implement and doesn't require complex configurations or data migrations.
 - 5. Retention of Performance Insights Data: Since the instance is only stopped, not terminated, you retain the Performance Insights data, which can be valuable for analyzing test results over time.
- Best practices and considerations:
 - 1. Automation: Consider using AWS Lambda functions triggered by Amazon CloudWatch Events to automatically stop the instance after the 48-hour test period and start it before the next testing cycle.
 - 2. Backup Strategy: Ensure you have a robust backup strategy in place, including automated backups and manual snapshots before stopping the instance.
 - 3. Security: When restarting the instance, always ensure it's launched within a secure VPC with appropriate security group rules.
 - 4. Monitoring: Set up CloudWatch alarms to monitor the instance status and any potential issues during the start/stop processes.
 - 5. Cost Tracking: Use AWS Cost Explorer or AWS Budgets to track the cost savings achieved through this approach. By implementing this solution, the development team can significantly reduce costs while maintaining the necessary performance for their monthly tests.
- Remember to consult the AWS documentation for the most up-to-date information on RDS instance management and pricing details.

Sources

- [1] [Improving query performance for RDS for MySQL with Amazon RDS Optimized Reads – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-optimized-reads.html>)
- [3] [Amazon RDS for

MySQL – Amazon Relational Database Service]
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQL.html)
[6] [Optimize cost and boost performance of RDS for MySQL using Amazon
ElastiCache for Redis | AWS Database Blog] (<https://aws.amazon.com/blogs/database/optimize-cost-and-boost-performance-of-rds-for-mysql-using-amazon-elasticache-for-redis/>) 投票多数的为C，但是此题建议选择A。
解析: To address the development team's requirement of reducing costs for their monthly resource-intensive tests on the Amazon RDS for MySQL DB instance without reducing compute and memory attributes, the most cost-effective solution is: A. Stop the DB instance when tests are completed. Restart the DB instance when required. This approach offers several benefits: 1. Cost Savings: When you stop an RDS instance, you only pay for the storage and any associated backups. You're not charged for the compute capacity while the instance is stopped, which can lead to significant cost savings, especially for a DB instance that's only used for 48 hours each month. 2. Maintains Instance Attributes: Stopping and starting the instance preserves all the compute and memory attributes, meeting the requirement not to reduce these resources. 3. Quick Availability: Restarting a stopped RDS instance is typically faster than creating a new instance from a snapshot, making the database available quickly when needed for the next testing cycle. 4. Simplicity: This solution is straightforward to implement and doesn't require complex configurations or data migrations. 5. Retention of Performance Insights Data: Since the instance is only stopped, not terminated, you retain the Performance Insights data, which can be valuable for analyzing test results over time. Best practices and considerations: 1. Automation: Consider using AWS Lambda functions triggered by Amazon CloudWatch Events to automatically stop the instance after the 48-hour test period and start it before the next testing cycle. 2. Backup Strategy: Ensure you have a robust backup strategy in place, including automated backups and manual snapshots before stopping the instance. 3. Security: When restarting the instance, always ensure it's launched within a secure VPC with appropriate security group rules. 4. Monitoring: Set up CloudWatch alarms to monitor the instance status and any potential issues during the

start/stop processes.

5. Cost Tracking: Use AWS Cost Explorer or AWS Budgets to track the cost savings achieved through this approach. By implementing this solution, the development team can significantly reduce costs while maintaining the necessary performance for their monthly tests. Remember to consult the AWS documentation for the most up-to-date information on RDS instance management and pricing details. Sources [1] [Improving query performance for RDS for MySQL with Amazon RDS Optimized Reads – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-optimized-reads.html>) [3] [Amazon RDS for MySQL – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_MySQL.html) [6] [Optimize cost and boost performance of RDS for MySQL using Amazon ElastiCache for Redis | AWS Database Blog] (<https://aws.amazon.com/blogs/database/optimize-cost-and-boost-performance-of-rds-for-mysql-using-amazon-elasticsearch-for-redis/>) 投票多数的为C，但是此题建议选择A。

29. Question #31 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?

- 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.

答案：A

解析：AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, including tagging. By creating Config rules, you can automate the process of identifying and

notifying about improperly tagged resources, which reduces the effort required for manual checks and updates.

解析: AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources, including tagging. By creating Config rules, you can automate the process of identifying and notifying about improperly tagged resources, which reduces the effort required for manual checks and updates.

30. Question #32 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?

- 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.

答案: B

解析: Amazon S3 is designed for storing and serving static content, which includes websites composed of HTML, CSS, JavaScript, and images. Hosting a website in S3 is generally more cost-effective than using compute resources like EC2 instances or container services like Fargate, as it does not incur ongoing compute charges.

解析: Amazon S3 is designed for storing and serving static content, which includes websites composed of HTML, CSS, JavaScript, and images. Hosting a website in S3 is generally more cost-effective than using compute resources like EC2 instances or container services like Fargate, as it does not incur ongoing compute charges.

31. Question #33 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?

- 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.

答案：C

解析：Amazon Kinesis Data Streams provides a scalable, real-time data processing service that can handle high throughput and low latency. By using Kinesis Data Streams, the company can stream the transaction data, process it with AWS Lambda to remove sensitive information, and then store the sanitized data in Amazon DynamoDB. This setup allows for near-real-time data sharing with other internal applications and ensures that sensitive data is removed before storage.

解析：Amazon Kinesis Data Streams provides a scalable, real-time data processing service that can handle high throughput and low latency. By using Kinesis Data Streams, the company can stream the transaction data, process it with AWS Lambda to remove sensitive information, and then store the sanitized data in Amazon DynamoDB. This setup allows for near-real-time data sharing with other internal applications and ensures that sensitive data is removed before storage.

32. Question #34 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?

- 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 AWS Config to track configuration changes and Amazon CloudWatch to record API calls.
- D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.

答案：B

解析：AWS Config is used to assess, audit, and evaluate the configurations of AWS resources, providing a detailed view of their configuration history. AWS CloudTrail, on the other hand, is a service that enables the recording of API calls made to AWS resources, providing a history of user activity and API call history. Together, these services fulfill the requirements for tracking configuration changes and recording API calls for compliance and security purposes.

解析：AWS Config is used to assess, audit, and evaluate the configurations of AWS resources, providing a detailed view of their configuration history. AWS CloudTrail, on the other hand, is a service that enables the recording of API calls made to AWS resources, providing a history of user activity and API call history. Together, these services fulfill the requirements for tracking configuration changes and recording API calls for compliance and security purposes.

33. Question #35A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions

architect must recommend a solution to detect and protect against large-scale DDoS attacks. Which solution meets these requirements?

- A. Enable Amazon GuardDuty on the account.
- B. Enable Amazon Inspector on the EC2 instances.
- C. Enable AWS Shield and assign Amazon Route 53 to it.
- D. Enable AWS Shield Advanced and assign the ELB to it.

答案: D

解析: AWS Shield Advanced provides expanded DDoS attack protection for resources such as Amazon EC2 instances, Elastic Load Balancing load balancers, and more. By enabling AWS Shield Advanced and assigning the ELB, the company can protect its web application against large-scale DDoS attacks, ensuring the application remains available during such events.

解析: AWS Shield Advanced provides expanded DDoS attack protection for resources such as Amazon EC2 instances, Elastic Load Balancing load balancers, and more. By enabling AWS Shield Advanced and assigning the ELB, the company can protect its web application against large-scale DDoS attacks, ensuring the application remains available during such events.

34. Question #36A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions. Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.
- B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.
- C. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3

managed encryption keys (SSE-S3). Configure replication between the S3 buckets.

D. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

答案：B

解析：By creating a multi-Region KMS key, the company can ensure that the same encryption key is available in both Regions, allowing for encryption and decryption of data in S3 buckets located in different Regions.

Configuring the application to use this KMS key for client-side encryption ensures that data is encrypted before it is sent to S3, providing an additional layer of security. 43%认为可能选择D。

解析：By creating a multi-Region KMS key, the company can ensure that the same encryption key is available in both Regions, allowing for encryption and decryption of data in S3 buckets located in different Regions.

Configuring the application to use this KMS key for client-side encryption ensures that data is encrypted before it is sent to S3, providing an additional layer of security. 43%认为可能选择D。

35. Question #37A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely.

The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework. Which solution will meet these requirements with the LEAST operational overhead?

A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.

B. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.

C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.

D. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

答案：B

解析：By attaching IAM roles to EC2 instances and using AWS Systems Manager Session Manager, the company can establish secure and auditable remote connections to the instances without the need to open inbound ports or manage SSH keys. This approach aligns with the AWS Well-Architected Framework and provides a repeatable, scalable, and secure method for administering EC2 instances.

解析：By attaching IAM roles to EC2 instances and using AWS Systems Manager Session Manager, the company can establish secure and auditable remote connections to the instances without the need to open inbound ports or manage SSH keys. This approach aligns with the AWS Well-Architected Framework and provides a repeatable, scalable, and secure method for administering EC2 instances.

36. Question #38 A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website. Which solution meets these requirements MOST cost-effectively?

- A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
- B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
- C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
- D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

答案：C

解析：Amazon CloudFront is a content delivery network (CDN) service that can significantly reduce latency by caching content at edge locations

around the world. By creating a CloudFront distribution in front of the S3 bucket and updating the Route 53 records to point to the CloudFront distribution, the company can ensure that users are served content from the nearest edge location, resulting in lower latency.

解析: Amazon CloudFront is a content delivery network (CDN) service that can significantly reduce latency by caching content at edge locations around the world. By creating a CloudFront distribution in front of the S3 bucket and updating the Route 53 records to point to the CloudFront distribution, the company can ensure that users are served content from the nearest edge location, resulting in lower latency.

37. Question #39 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?

- 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.

答案: A

解析: General Purpose SSD storage is not optimized for high I/O performance. By switching to Provisioned IOPS SSD storage, the company can reserve IOPS for the database, which is designed to provide high and consistent I/O performance, ideal for heavy write workloads like the one described.

解析: General Purpose SSD storage is not optimized for high I/O performance. By switching to Provisioned IOPS SSD storage, the company can reserve IOPS for the database, which is designed to provide high and consistent I/O performance, ideal for heavy write workloads like the one

described.

38. Question #40 A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis. The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure.

Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.
- D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

答案：A

解析: Amazon Kinesis Data Firehose is a fully managed service that can automatically ingest and load streaming data to destinations like Amazon S3. By setting up a delivery stream with Kinesis Data Firehose, the company can offload the data ingestion and storage operations to a managed service, reducing the need for managing infrastructure.

Configuring S3 Lifecycle to transition data to Amazon S3 Glacier after 14 days ensures that older data is archived at a lower cost while still being available for future analysis.

解析: Amazon Kinesis Data Firehose is a fully managed service that can automatically ingest and load streaming data to destinations like Amazon S3. By setting up a delivery stream with Kinesis Data Firehose, the company can offload the data ingestion and storage operations to a managed service, reducing the need for managing infrastructure.

Configuring S3 Lifecycle to transition data to Amazon S3 Glacier after 14 days ensures that older data is archived at a lower cost while still being available for future analysis.

39. Question #41A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible. Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Auto Scaling group so that EC2 instances can scale out.

Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

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

- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (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.

答案：B

解析：Amazon AppFlow is a fully managed integration service that simplifies the process of securely transferring data between SaaS applications and AWS services like Amazon S3. By using AppFlow, the company can automate the data transfer process without the need for managing EC2 instances, reducing operational overhead and improving application performance.

解析：Amazon AppFlow is a fully managed integration service that simplifies the process of securely transferring data between SaaS applications and AWS services like Amazon S3. By using AppFlow, the company can automate the data transfer process without the need for managing EC2 instances, reducing operational overhead and improving application performance.

40. Question #42 A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges. What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

- A. Launch the NAT gateway in each Availability Zone.

- B. Replace the NAT gateway with a NAT instance.
- C. Deploy a gateway VPC endpoint for Amazon S3.
- D. Provision an EC2 Dedicated Host to run the EC2 instances.

答案：C

解析：VPC endpoints for Amazon S3 allow for private connectivity between the VPC and S3 without the need for a NAT gateway or an Internet gateway. This means that all data transfers between the VPC and S3 occur within the AWS network, avoiding Regional data transfer charges. Using a gateway VPC endpoint for Amazon S3 is the most cost-effective solution to prevent these charges.

解析：VPC endpoints for Amazon S3 allow for private connectivity between the VPC and S3 without the need for a NAT gateway or an Internet gateway. This means that all data transfers between the VPC and S3 occur within the AWS network, avoiding Regional data transfer charges. Using a gateway VPC endpoint for Amazon S3 is the most cost-effective solution to prevent these charges.

41. Question #43 A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users. Which solution meets these requirements?

- A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
- B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
- C. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.
- D. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

答案：B

解析: AWS Direct Connect provides a dedicated network connection from the on-premises environment to AWS, which can significantly increase the bandwidth for data transfers and reduce the load on the internet connectivity. By directing backup traffic through an AWS Direct Connect connection, the company can ensure that the backups to S3 are performed quickly and with minimal impact on the internal network usage.

解析: AWS Direct Connect provides a dedicated network connection from the on-premises environment to AWS, which can significantly increase the bandwidth for data transfers and reduce the load on the internet connectivity. By directing backup traffic through an AWS Direct Connect connection, the company can ensure that the backups to S3 are performed quickly and with minimal impact on the internal network usage.

42. Question #46A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size. Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation. What should a solutions architect do to meet these requirements with the LEAST development effort?

- A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.
- B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to

trigger a notification to the administrators to remove the objects that contain PII.

D. Implement custom scanning algorithms in an AWS Lambda function.

Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the objects that contain PII.

答案：B

解析：Amazon Macie is a data security and data privacy service that uses machine learning to automatically discover, classify, and protect sensitive data. By using an S3 bucket as a secure transfer point and subscribing the S3 bucket to an Amazon Macie service, the company can scan the objects for PII with minimal development effort. If Macie detects PII in the objects, it can trigger an Amazon SNS notification to alert administrators, who can then take action to remove the objects containing PII. This approach automates the detection and notification process, requiring less development effort compared to implementing custom scanning algorithms in a Lambda function.

解析：Amazon Macie is a data security and data privacy service that uses machine learning to automatically discover, classify, and protect sensitive data. By using an S3 bucket as a secure transfer point and subscribing the S3 bucket to an Amazon Macie service, the company can scan the objects for PII with minimal development effort. If Macie detects PII in the objects, it can trigger an Amazon SNS notification to alert administrators, who can then take action to remove the objects containing PII. This approach automates the detection and notification process, requiring less development effort compared to implementing custom scanning algorithms in a Lambda function.

43. Question #47A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week. What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved Instances that specify the Region needed.

- B. Create an On-Demand Capacity Reservation that specifies the Region needed.
- C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
- D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

答案: D

解析: On-Demand Capacity Reservations in Amazon EC2 allow customers to reserve capacity for On-Demand instances in specific Availability Zones. By creating an On-Demand Capacity Reservation that specifies the Region and three Availability Zones, the company can guarantee the EC2 capacity it needs for the event. This is a more suitable option than purchasing Reserved Instances, which are typically used for long-term commitments and do not guarantee capacity in specific Availability Zones.

解析: On-Demand Capacity Reservations in Amazon EC2 allow customers to reserve capacity for On-Demand instances in specific Availability Zones. By creating an On-Demand Capacity Reservation that specifies the Region and three Availability Zones, the company can guarantee the EC2 capacity it needs for the event. This is a more suitable option than purchasing Reserved Instances, which are typically used for long-term commitments and do not guarantee capacity in specific Availability Zones.

44. Question #48A 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 that the catalog is stored in a durable location. What should a solutions architect do to meet these requirements?

- 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.

答案: D

解析: Amazon EFS is designed to be highly durable and highly available, making it a suitable storage solution for data that needs to be accessed concurrently from multiple Amazon EC2 instances. By moving the catalog to an Amazon EFS file system, the company can ensure that the catalog is stored in a durable location and is highly available for access by the website. Amazon ElastiCache for Redis is an in-memory cache service, not a storage service, and is not suitable for durable storage. Amazon S3 Glacier Deep Archive is designed for long-term, infrequent access, which does not meet the requirement for high availability.

解析: Amazon EFS is designed to be highly durable and highly available, making it a suitable storage solution for data that needs to be accessed concurrently from multiple Amazon EC2 instances. By moving the catalog to an Amazon EFS file system, the company can ensure that the catalog is stored in a durable location and is highly available for access by the website. Amazon ElastiCache for Redis is an in-memory cache service, not a storage service, and is not suitable for durable storage. Amazon S3 Glacier Deep Archive is designed for long-term, infrequent access, which does not meet the requirement for high availability.

45. Question #49A 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?

- A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
- 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 the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.

C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.

D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

答案：B

解析：Amazon S3 Intelligent-Tiering is an storage class that automatically moves data to the most cost-effective storage tier based on access patterns. This makes it ideal for data with unpredictable access patterns. By storing the files in S3 Intelligent-Tiering and using S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year, the company can ensure quick access to files less than 1 year old while optimizing costs for older files. Amazon Athena and S3 Glacier Select can be used to query and retrieve files from S3 and S3 Glacier respectively. This solution balances cost-effectiveness with the need for quick retrieval of recent files.

解析：Amazon S3 Intelligent-Tiering is an storage class that automatically moves data to the most cost-effective storage tier based on access patterns. This makes it ideal for data with unpredictable access patterns. By storing the files in S3 Intelligent-Tiering and using S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year, the company can ensure quick access to files less than 1 year old while optimizing costs for older files. Amazon Athena and S3 Glacier Select can be used to query and retrieve files from S3 and S3 Glacier respectively. This solution balances cost-effectiveness with the need for quick retrieval of recent files.

46. Question #50A 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?

- 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.

答案：D

解析：AWS Systems Manager Run Command allows the execution of commands or scripts on multiple EC2 instances. By using Run Command, the architect can quickly apply the patch to all 1,000 EC2 instances, addressing the critical security vulnerability. This approach is more suitable than creating a Lambda function, which is not designed to run on EC2 instances, or scheduling a maintenance window, which may not be as quick. Patch Manager is designed for ongoing patch management rather than urgent patching, making Run Command the best choice for this scenario.

解析：AWS Systems Manager Run Command allows the execution of commands or scripts on multiple EC2 instances. By using Run Command, the architect can quickly apply the patch to all 1,000 EC2 instances, addressing the critical security vulnerability. This approach is more suitable than creating a Lambda function, which is not designed to run on EC2 instances, or scheduling a maintenance window, which may not be as quick. Patch Manager is designed for ongoing patch management rather than urgent patching, making Run Command the best choice for this scenario.

47. Question #52A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead. Which solution will meet these requirements?

- A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.
- B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.
- C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
- D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

答案: C

解析: Amazon EFS is a scalable, resilient file storage service that is ideal for applications that require a standard file system structure. By migrating the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group and using Amazon EFS for storage, the company can ensure that the application scales automatically, remains highly available, and requires minimal operational overhead.

解析: Amazon EFS is a scalable, resilient file storage service that is ideal for applications that require a standard file system structure. By migrating the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group and using Amazon EFS for storage, the company can ensure that the application scales automatically, remains highly available, and requires minimal operational overhead.

48. Question #53A 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?

- 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.

- 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.

答案: C

解析: To meet the requirements, the company can use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year, which is designed for long-term retention of data that is accessed rarely. Using S3 Object Lock in compliance mode for a period of 10 years ensures that the records cannot be deleted by anyone, including administrative users and root users, during the entire 10-year period. This solution provides maximum resiliency and meets the requirements for immediate accessibility and long-term archiving.

解析: To meet the requirements, the company can use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year, which is designed for long-term retention of data that is accessed rarely. Using S3 Object Lock in compliance mode for a period of 10 years ensures that the records cannot be deleted by anyone, including administrative users and root users, during the entire 10-year period. This solution provides maximum resiliency and meets the requirements for immediate accessibility and long-term archiving.

49. Question #54A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files. What should a solutions architect do to meet these requirements?
- A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.
 - B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.

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

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

答案: C

解析: Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. By extending the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration, the company can maintain the same access methods for users while achieving high availability and durability. This solution preserves the current way users access the files and provides a more resilient storage solution than Amazon EFS, which is not natively compatible with Windows.

解析: Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. By extending the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration, the company can maintain the same access methods for users while achieving high availability and durability. This solution preserves the current way users access the files and provides a more resilient storage solution than Amazon EFS, which is not natively compatible with Windows.

50. Question #55A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS DB instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases. Which solution will meet these requirements?

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

subnets.

- B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
- C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

答案：C

解析：To restrict access to the RDS databases to only EC2 instances running in the private subnets, the architect should create a security group that allows inbound traffic from the security group assigned to instances in the private subnets (Option C). This security group can then be attached to the DB instances, ensuring that only the specified instances have access to the databases. Creating a route table that excludes routes to the public subnets (Option A) or configuring peering connections (Option D) does not directly address the requirement for controlling access to the databases. Denying inbound traffic from the public subnets' security group (Option B) would prevent all traffic, not just from the public subnets, from reaching the DB instances.

解析：To restrict access to the RDS databases to only EC2 instances running in the private subnets, the architect should create a security group that allows inbound traffic from the security group assigned to instances in the private subnets (Option C). This security group can then be attached to the DB instances, ensuring that only the specified instances have access to the databases. Creating a route table that excludes routes to the public subnets (Option A) or configuring peering connections (Option D) does not directly address the requirement for controlling access to the databases. Denying inbound traffic from the public subnets' security group (Option B) would prevent all traffic, not just from the public subnets, from reaching the DB instances.

51. Question #56A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS. Which solution will meet these requirements?

- A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
- C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.
- D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

答案: C

解析: To configure the API Gateway URL with the company's domain name and to use HTTPS, the architect should create a Regional API Gateway endpoint and associate it with the company's domain name. The public certificate for the domain should be imported into AWS Certificate Manager (ACM) in the same Region as the API Gateway endpoint and then attached to the API Gateway. Finally, Route 53 should be configured to route traffic to the

API Gateway endpoint using the company's domain name. This solution ensures secure communication with the APIs and allows third-party services to consume them using HTTPS.

解析: To configure the API Gateway URL with the company's domain name and to use HTTPS, the architect should create a Regional API Gateway endpoint and associate it with the company's domain name. The public certificate for the domain should be imported into AWS Certificate Manager (ACM) in the same Region as the API Gateway endpoint and then attached to the API Gateway. Finally, Route 53 should be configured to route traffic to the API Gateway endpoint using the company's domain name. This solution ensures secure communication with the APIs and allows third-party services to consume them using HTTPS.

52. Question #57A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort. What should a solutions architect do to meet these requirements?

- A. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.
- B. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.
- C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.
- D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

答案: B

解析: Amazon Rekognition is a service that provides object and scene detection in images and videos. It can be used to detect inappropriate content in images with high accuracy, which requires minimal development effort. For cases where the confidence of the detection is low, a human review can be used to make the final decision. This solution is efficient

and reduces the need for custom machine learning models or extensive development work.

解析: Amazon Rekognition is a service that provides object and scene detection in images and videos. It can be used to detect inappropriate content in images with high accuracy, which requires minimal development effort. For cases where the confidence of the detection is low, a human review can be used to make the final decision. This solution is efficient and reduces the need for custom machine learning models or extensive development work.

53. Question #58A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload. What should a solutions architect do to meet these requirements?

- A. Use Amazon EC2 instances, and install Docker on the instances.
- B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

答案: C

解析: AWS Fargate is a serverless compute engine for containers that allows developers to focus on building applications without the need to manage servers or clusters. By using Amazon ECS on AWS Fargate, the company can run its critical applications in containers while AWS manages the infrastructure. This solution provides scalability and availability without the overhead of infrastructure management.

解析: AWS Fargate is a serverless compute engine for containers that allows developers to focus on building applications without the need to manage servers or clusters. By using Amazon ECS on AWS Fargate, the company can run its critical applications in containers while AWS manages the infrastructure. This solution provides scalability and availability

without the overhead of infrastructure management.

54. Question #59A 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?

- 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.

答案: D

解析: Amazon Kinesis Data Streams can collect and process large streams of data in real-time. By using Kinesis Data Streams to collect the clickstream data, the company can ensure that the data is transmitted and processed efficiently. Amazon Kinesis Data Firehose can then be used to transmit the data to an S3 data lake, where it can be loaded into Amazon Redshift for analysis. This solution provides a scalable and reliable way to handle the large volume of clickstream data.

解析: Amazon Kinesis Data Streams can collect and process large streams of data in real-time. By using Kinesis Data Streams to collect the clickstream data, the company can ensure that the data is transmitted and processed efficiently. Amazon Kinesis Data Firehose can then be used to transmit the data to an S3 data lake, where it can be loaded into Amazon Redshift for analysis. This solution provides a scalable and reliable way to handle the large volume of clickstream data.

55. Question #60A 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?

- 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).

答案：C

解析：To ensure that all requests to the website use HTTPS, the architect should create a listener rule on the ALB that redirects HTTP traffic to HTTPS. This solution automatically redirects incoming HTTP requests to the HTTPS listener, ensuring secure communication without requiring any changes to the website's URL.

解析：To ensure that all requests to the website use HTTPS, the architect should create a listener rule on the ALB that redirects HTTP traffic to HTTPS. This solution automatically redirects incoming HTTP requests to the HTTPS listener, ensuring secure communication without requiring any changes to the website's URL.

56. Question #61A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis. Which solution will meet these requirements with the LEAST operational overhead?

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

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

C. Store the database credentials as a secret in AWS Secrets Manager.

Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

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

答案：C

解析：AWS Secrets Manager is a service designed to manage secrets, such as database credentials, with ease. By storing the credentials as a secret and enabling automatic rotation, the company can ensure that the credentials are regularly updated without manual intervention. Attaching the necessary permissions to the EC2 role allows the application to access the secrets as needed. This solution provides a secure and operationally efficient way to manage and rotate database credentials.

解析：AWS Secrets Manager is a service designed to manage secrets, such as database credentials, with ease. By storing the credentials as a secret and enabling automatic rotation, the company can ensure that the credentials are regularly updated without manual intervention. Attaching the necessary permissions to the EC2 role allows the application to access the secrets as needed. This solution provides a secure and operationally efficient way to manage and rotate database credentials.

57. Question #62A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires. What should a solutions architect do to meet these requirements?

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

答案: D

解析: Since the certificate is being issued by an external CA, it must be imported into AWS Certificate Manager (ACM). ACM does not support automatic renewal of imported certificates, so the company must monitor the expiration date and manually rotate the certificate. Using Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration is a useful strategy to ensure timely rotation without manual monitoring.

解析: Since the certificate is being issued by an external CA, it must be imported into AWS Certificate Manager (ACM). ACM does not support automatic renewal of imported certificates, so the company must monitor the expiration date and manually rotate the certificate. Using Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration is a useful strategy to ensure timely rotation without manual monitoring.

58. Question #63A 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?

- 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 .pdffiles 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.

答案：A

解析：Using Amazon S3 to store the original .pdf files and configuring S3 PUT events to trigger AWS Lambda functions for the conversion to .jpg format is a cost-effective solution. This approach leverages the scalability and pay-as-you-go pricing of both S3 and Lambda, making it suitable for handling large volumes of data and accommodating rapid growth in demand.

解析：Using Amazon S3 to store the original .pdf files and configuring S3 PUT events to trigger AWS Lambda functions for the conversion to .jpg format is a cost-effective solution. This approach leverages the scalability and pay-as-you-go pricing of both S3 and Lambda, making it suitable for handling large volumes of data and accommodating rapid growth in demand.

59. Question #64A 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?

- 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.

答案: D

解析: The solution that meets the requirements of minimum latency and no significant changes to existing file access patterns is to deploy Amazon FSx for Windows File Server on AWS and an Amazon FSx File Gateway on premises. This setup allows the company to move the on-premises file data to the FSx File Gateway and maintain the same file access patterns for users and applications. The AWS Site-to-Site VPN connection ensures secure and seamless connectivity between the on-premises and AWS environments.

解析: The solution that meets the requirements of minimum latency and no significant changes to existing file access patterns is to deploy Amazon FSx for Windows File Server on AWS and an Amazon FSx File Gateway on premises. This setup allows the company to move the on-premises file data to the FSx File Gateway and maintain the same file access patterns for users and applications. The AWS Site-to-Site VPN connection ensures secure and seamless connectivity between the on-premises and AWS environments.

60. Question #65A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
- B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.
- C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
- D. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

答案: C

解析: Amazon Textract is specifically designed to extract text and data from scanned documents, including PDFs and JPEGs. Amazon Comprehend Medical is a service that can identify and protect PHI within the text. By using Textract to extract the text and Comprehend Medical to identify PHI, the hospital can efficiently and accurately process the reports with minimal operational overhead.

解析: Amazon Textract is specifically designed to extract text and data from scanned documents, including PDFs and JPEGs. Amazon Comprehend Medical is a service that can identify and protect PHI within the text. By using Textract to extract the text and Comprehend Medical to identify

PHI, the hospital can efficiently and accurately process the reports with minimal operational overhead.

61. Question #66A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days. Which storage solution is MOST cost-effective?

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

答案: C

解析: Given that the files are frequently accessed in the first 30 days and then rarely accessed but still require immediate accessibility, the most cost-effective solution is to use S3 Standard-Infrequent Access (S3 Standard-IA). This storage class provides lower costs than S3 Standard for data that is accessed less frequently but still requires high durability and immediate availability. The files can be stored in S3 Standard-IA for the entire 4-year period without the need to move them to S3 Glacier, which would incur additional retrieval costs and potentially longer retrieval times.

解析: Given that the files are frequently accessed in the first 30 days and then rarely accessed but still require immediate accessibility, the most cost-effective solution is to use S3 Standard-Infrequent Access (S3 Standard-IA). This storage class provides lower costs than S3 Standard for data that is accessed less frequently but still requires high durability and immediate availability. The files can be stored in S3 Standard-IA for the entire 4-year period without the need to move them to S3 Glacier, which would incur additional retrieval costs and potentially longer retrieval times.

62. Question #67A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?
- A. Use the CreateQueue API call to create a new queue.
 - B. Use the AddPermission API call to add appropriate permissions.
 - C. Use the ReceiveMessage API call to set an appropriate wait time.
 - D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

答案: D

解析: To ensure that messages are processed once, the visibility timeout of the messages in the SQS queue should be set appropriately. By using the ChangeMessageVisibility API call to increase the visibility timeout, the architect can ensure that a message is not visible to other consumers while it is being processed. This prevents other consumers from picking up and processing the same message, thus avoiding duplicate records in the RDS table.

解析: To ensure that messages are processed once, the visibility timeout of the messages in the SQS queue should be set appropriately. By using the ChangeMessageVisibility API call to increase the visibility timeout, the architect can ensure that a message is not visible to other consumers while it is being processed. This prevents other consumers from picking

up and processing the same message, thus avoiding duplicate records in the RDS table.

63. Question #68A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails. What should the solutions architect do to meet these requirements?

- A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
- B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
- C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
- D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

答案：A

解析：AWS Direct Connect provides a dedicated network connection from the company's on-premises infrastructure to AWS, offering consistent low latency and high availability. By provisioning a Direct Connect connection as the primary connection and a VPN connection as a backup, the architect can ensure that the company has a highly available and low-latency connection to AWS while also minimizing costs. The VPN connection can serve as a fallback option in case the Direct Connect connection fails, providing slower traffic but ensuring continued connectivity.

解析：AWS Direct Connect provides a dedicated network connection from the company's on-premises infrastructure to AWS, offering consistent low latency and high availability. By provisioning a Direct Connect

connection as the primary connection and a VPN connection as a backup, the architect can ensure that the company has a highly available and low-latency connection to AWS while also minimizing costs. The VPN connection can serve as a fallback option in case the Direct Connect connection fails, providing slower traffic but ensuring continued connectivity.

64. Question #69A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data. Which solution will meet these requirements with the LEAST operational effort?

- A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.
- B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
- C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.
- D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

答案: B

解析: Based on the company's requirements for a highly available business-critical web application with minimum downtime and data loss, the best solution with the least operational effort is: 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. Here's why this solution is recommended: 1. High Availability:

- Using multiple Availability Zones (AZs) for the Auto Scaling group

ensures that the EC2 instances are distributed across different AZs, providing redundancy and fault tolerance.

- Configuring the Aurora PostgreSQL database as Multi-AZ creates a standby replica in a different AZ, allowing for automatic failover in case of an outage.

2. Minimum Downtime:

- The Application Load Balancer will distribute traffic across healthy instances in multiple AZs, ensuring continuous service even if one AZ experiences issues.
- Multi-AZ configuration for the database allows for quick failover to the standby replica, minimizing downtime during database failures.

3. Minimum Data Loss:

- Multi-AZ deployment for Aurora PostgreSQL provides synchronous replication, ensuring that data is consistently updated across both the primary and standby instances.

4. Least Operational Effort:

- Auto Scaling and Multi-AZ configurations are managed by AWS, reducing the operational overhead for the company.
- Amazon RDS Proxy provides connection pooling and automatic failover, further reducing management complexity.

Implementation steps and best practices:

1. Configure the Auto Scaling group:
 - Select at least two Availability Zones in the region.
 - Set appropriate minimum, desired, and maximum capacity.
 - Configure health checks to ensure only healthy instances receive traffic.
2. Set up the Aurora PostgreSQL database:
 - Enable Multi-AZ deployment during database creation or modify an existing instance.
 - Ensure proper subnet configuration in different AZs for the primary and standby instances
3. Implement Amazon RDS Proxy:
 - Create an RDS Proxy instance for the Aurora PostgreSQL database.
 - Configure the proxy endpoint in your application instead of directly connecting to the database.
4. Security considerations:
 - Use security groups to control access between the EC2 instances, RDS Proxy, and the database.
 - Implement the principle of least privilege for IAM roles associated with EC2 instances and RDS Proxy.
5. Monitoring and maintenance:
 - Set up Amazon CloudWatch alarms to monitor the health and performance of EC2 instances, the database, and the RDS Proxy.
 - Regularly review and update your Auto Scaling policies based on application demand patterns.

ref: [1] [Auto Scaling benefits for application architecture – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/>)

[auto-scaling-benefits.html](#)) [3] [Resilience in Amazon EC2 Auto Scaling – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/useguide/disaster-recovery-resiliency.html>) [6] [Tutorial: Set up a scaled and load-balanced application – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/tutorial-ec2-auto-scaling-load-balancer.html>)

解析: Based on the company's requirements for a highly available business-critical web application with minimum downtime and data loss, the best solution with the least operational effort is: 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. Here's why this solution is recommended:

1. High Availability:

- Using multiple Availability Zones (AZs) for the Auto Scaling group ensures that the EC2 instances are distributed across different AZs, providing redundancy and fault tolerance.
- Configuring the Aurora PostgreSQL database as Multi-AZ creates a standby replica in a different AZ, allowing for automatic failover in case of an outage.

2. Minimum Downtime:

- The Application Load Balancer will distribute traffic across healthy instances in multiple AZs, ensuring continuous service even if one AZ experiences issues.
- Multi-AZ configuration for the database allows for quick failover to the standby replica, minimizing downtime during database failures.

3. Minimum Data Loss:

- Multi-AZ deployment for Aurora PostgreSQL provides synchronous replication, ensuring that data is consistently updated across both the primary and standby instances.
- 4. Least Operational Effort:

- Auto Scaling and Multi-AZ configurations are managed by AWS, reducing the operational overhead for the company.
- Amazon RDS Proxy provides connection pooling and automatic failover, further reducing management complexity.

Implementation steps and best practices:

1. Configure the Auto Scaling group:

- Select at least two Availability Zones in the region.
- Set appropriate minimum, desired, and maximum capacity.
- Configure health checks to ensure only healthy instances receive traffic.

 2. Set up the Aurora PostgreSQL database:

 - Enable Multi-AZ deployment during database creation or modify an existing instance.
 - Ensure proper

subnet configuration in different AZs for the primary and standby instances 3. Implement Amazon RDS Proxy: – Create an RDS Proxy instance for the Aurora PostgreSQL database. – Configure the proxy endpoint in your application instead of directly connecting to the database. 4. Security considerations: – Use security groups to control access between the EC2 instances, RDS Proxy, and the database. – Implement the principle of least privilege for IAM roles associated with EC2 instances and RDS Proxy. 5. Monitoring and maintenance: – Set up Amazon CloudWatch alarms to monitor the health and performance of EC2 instances, the database, and the RDS Proxy. – Regularly review and update your Auto Scaling policies based on application demand patterns.

ref: [1] [Auto Scaling benefits for application architecture – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>) [3] [Resilience in Amazon EC2 Auto Scaling – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/useguide/disaster-recovery-resiliency.html>) [6] [Tutorial: Set up a scaled and load-balanced application – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/tutorial-ec2-auto-scaling-load-balancer.html>)

65. Question #76A 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?

- 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

答案: B

解析: AWS DataSync is a data transfer service that can be optimized for transferring data efficiently and securely between on-premises storage systems and Amazon S3. When used over AWS Direct Connect, DataSync can provide a dedicated and secure network connection, ensuring a more reliable data transfer compared to using the public internet. AWS DMS is primarily designed for database migration and may not be as efficient for transferring large amounts of JSON files.

解析: AWS DataSync is a data transfer service that can be optimized for transferring data efficiently and securely between on-premises storage systems and Amazon S3. When used over AWS Direct Connect, DataSync can provide a dedicated and secure network connection, ensuring a more reliable data transfer compared to using the public internet. AWS DMS is primarily designed for database migration and may not be as efficient for transferring large amounts of JSON files.

66. Question #77A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data. Which solution will meet these requirements with the LEAST operational overhead?

- A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
- C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.

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

答案：C

解析：Using Amazon API Gateway to create an API for data ingestion and Amazon Kinesis Data Firehose for real-time data streaming and storage in Amazon S3 provides a fully managed solution with minimal operational overhead. AWS Lambda functions can be triggered by Kinesis Data Firehose to transform the data as it is streamed. This solution leverages managed services and does not require managing an EC2 instance, reducing the operational overhead.

解析：Using Amazon API Gateway to create an API for data ingestion and Amazon Kinesis Data Firehose for real-time data streaming and storage in Amazon S3 provides a fully managed solution with minimal operational overhead. AWS Lambda functions can be triggered by Kinesis Data Firehose to transform the data as it is streamed. This solution leverages managed services and does not require managing an EC2 instance, reducing the operational overhead.

67. Question #78A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years. What is the MOST operationally efficient solution that meets these requirements?

- A. Use DynamoDB point-in-time recovery to back up the table continuously.
- B. Use AWS Backup to create backup schedules and retention policies for the table.
- C. Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

答案：B

解析: AWS Backup is a service that simplifies and centralizes the backup of AWS resources, including DynamoDB tables. By using AWS Backup, the company can create backup schedules and retention policies that ensure the data is retained for the required 7 years. This solution is operationally efficient as it automates the backup process and requires minimal setup and management.

解析: AWS Backup is a service that simplifies and centralizes the backup of AWS resources, including DynamoDB tables. By using AWS Backup, the company can create backup schedules and retention policies that ensure the data is retained for the required 7 years. This solution is operationally efficient as it automates the backup process and requires minimal setup and management.

68. Question #79A 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?

- 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.

答案: A

解析: DynamoDB's on-demand capacity mode is the most cost-effective option for workloads with unpredictable traffic patterns. This mode automatically scales read and write capacity to handle the workload without the need for manual capacity planning. The company pays only for the capacity used, with no minimum fees or upfront costs, making it suitable for a table that is not used consistently throughout the day.

解析: DynamoDB's on-demand capacity mode is the most cost-effective option for workloads with unpredictable traffic patterns. This mode automatically scales read and write capacity to handle the workload without the need for manual capacity planning. The company pays only for

the capacity used, with no minimum fees or upfront costs, making it suitable for a table that is not used consistently throughout the day.

69. Question #80A 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?
- 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.

答案：B

解析：The most secure way to share the AMI is to modify the launchPermission property of the AMI to allow sharing only with the MSP Partner's AWS account. This ensures that the AMI is not publicly available or accessible to unauthorized accounts. Additionally, modifying the key policy to allow the MSP Partner's AWS account to use the existing KMS key for decrypting the EBS volume snapshots maintains the security of the encrypted data.

解析：The most secure way to share the AMI is to modify the launchPermission property of the AMI to allow sharing only with the MSP Partner's AWS account. This ensures that the AMI is not publicly

available or accessible to unauthorized accounts. Additionally, modifying the key policy to allow the MSP Partner's AWS account to use the existing KMS key for decrypting the EBS volume snapshots maintains the security of the encrypted data.

70. Question #81A 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?

- 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.

答案：C

解析：Using Amazon SQS as the job queue ensures that the job items are durably stored and can be processed in parallel by multiple application nodes. The processor application can be stateless, running on EC2 instances that are managed by an Auto Scaling group. By creating a launch template for the EC2 instances and configuring the Auto Scaling group to scale based on the number of items in the SQS queue, the architect can ensure that the application is loosely coupled and can handle varying workloads efficiently.

解析：Using Amazon SQS as the job queue ensures that the job items are durably stored and can be processed in parallel by multiple application nodes. The processor application can be stateless, running on EC2 instances that are managed by an Auto Scaling group. By creating a launch template for the EC2 instances and configuring the Auto Scaling group to scale based on the number of items in the SQS queue, the architect can ensure that the application is loosely coupled and can handle varying workloads efficiently.

71. Question #82A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate. What should a solutions architect recommend to meet this requirement?

- A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.
- B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
- C. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on

Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

答案：B

解析：AWS Config is a service that can monitor and evaluate AWS resource configurations against desired standards. By creating a rule in AWS Config to check for ACM certificates expiring within 30 days, the architect can set up Amazon EventBridge to trigger a custom alert via Amazon SNS when such a condition is met. This solution automates the process of notifying the security team about expiring certificates and ensures compliance with the company's requirements.

解析：AWS Config is a service that can monitor and evaluate AWS resource configurations against desired standards. By creating a rule in AWS Config to check for ACM certificates expiring within 30 days, the architect can set up Amazon EventBridge to trigger a custom alert via Amazon SNS when such a condition is met. This solution automates the process of notifying the security team about expiring certificates and ensures compliance with the company's requirements.

72. Question #83A 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?

- 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.

答案: C

解析: Amazon CloudFront is a content delivery network (CDN) service that can cache and distribute content from a custom origin, such as the company's on-premises servers in the United States, to edge locations closer to the European users. This solution reduces latency and improves site loading times without the need to migrate the backend or rearchitect the entire website. It provides an immediate way to optimize the user experience for the new European users.

解析: Amazon CloudFront is a content delivery network (CDN) service that can cache and distribute content from a custom origin, such as the company's on-premises servers in the United States, to edge locations closer to the European users. This solution reduces latency and improves site loading times without the need to migrate the backend or rearchitect the entire website. It provides an immediate way to optimize the user experience for the new European users.

73. Question #84A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours. The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use. Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

- A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
- B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.
- C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.

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

答案: B

解析: For the production environment, which requires 24/7 availability, using Reserved Instances is the most cost-effective option as it provides a significant discount compared to On-Demand Instances. For the development and test environments, which have variable usage and can be stopped during non-use periods, using On-Demand Instances is more suitable. This approach ensures that the company pays only for the compute resources it actually uses during development and testing, without incurring additional costs for reserved capacity.

解析: For the production environment, which requires 24/7 availability, using Reserved Instances is the most cost-effective option as it provides a significant discount compared to On-Demand Instances. For the development and test environments, which have variable usage and can be stopped during non-use periods, using On-Demand Instances is more suitable. This approach ensures that the company pays only for the compute resources it actually uses during development and testing, without incurring additional costs for reserved capacity.

74. Question #85A 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?

- 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.

答案: A

解析: To meet the regulatory requirement of preventing modification or deletion of documents after they are stored, the solutions architect should enable S3 Versioning and S3 Object Lock on the Amazon S3 bucket. S3 Versioning allows for the preservation of every version of the document, and S3 Object Lock provides a way to retain objects for a fixed period or indefinitely, ensuring that they cannot be deleted or overwritten.

解析: To meet the regulatory requirement of preventing modification or deletion of documents after they are stored, the solutions architect should enable S3 Versioning and S3 Object Lock on the Amazon S3 bucket. S3 Versioning allows for the preservation of every version of the document, and S3 Object Lock provides a way to retain objects for a fixed period or indefinitely, ensuring that they cannot be deleted or overwritten.

75. Question #86A 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?

- 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.

答案: A

解析: AWS Secrets Manager is a service specifically designed for managing secrets, such as database credentials. It allows for the secure storage of credentials and provides automated rotation of secrets, ensuring that the credentials are always fresh and secure. This meets the company's requirements for secure access to the database and frequent credential rotation.

解析: AWS Secrets Manager is a service specifically designed for managing secrets, such as database credentials. It allows for the secure storage of credentials and provides automated rotation of secrets, ensuring that the credentials are always fresh and secure. This meets the company's requirements for secure access to the database and frequent credential rotation.

76. Question #87A 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?

- 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.

答案: D

解析: Storing customer data in an Amazon SQS FIFO queue ensures that the data is preserved even if the database is temporarily unavailable during an upgrade. A Lambda function can be set up to poll the queue and store the data in the database once the upgrade is complete. This solution provides a reliable way to handle customer data during database maintenance without losing any data.

解析: Storing customer data in an Amazon SQS FIFO queue ensures that the data is preserved even if the database is temporarily unavailable during an upgrade. A Lambda function can be set up to poll the queue and store the data in the database once the upgrade is complete. This solution provides a reliable way to handle customer data during database maintenance without losing any data.

77. Question #88A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible. Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

答案: A

解析: To minimize data transfer costs for sharing data between the survey company in the United States and the European marketing firm, the best solution is: A. Configure the Requester Pays feature on the company's S3 bucket. Here's an overview of how to implement this solution and why it's the most cost-effective option:
1. Enable Requester Pays on the S3 bucket.

- Log in to the AWS Management Console and navigate to the S3 service.
- Select the bucket containing the survey data.
- Go to the

"Properties" tab. – Scroll down to the "Requester Pays" section and enable it. 2. Configure access permissions – In the bucket's "Permissions" tab, update the bucket policy to allow the marketing firm's AWS account to access the objects. – Ensure the principle of least privilege is applied by granting only necessary permissions. 3. Provide access information to the marketing firm – Share the bucket name and region with the European marketing firm. – Instruct them on how to access the data using their own AWS credentials. 4. Verify and monitor usage – Use AWS CloudTrail and S3 server access logging to monitor access to the bucket. – Regularly review access patterns and costs to ensure the arrangement is working as expected. This solution is optimal because:

- It keeps the data in a single location, avoiding duplication and synchronization issues.
- The marketing firm pays for the data transfer and request costs, reducing expenses for the survey company.
- It's simple to set up and doesn't require ongoing management of replication or sync processes.
- It allows for real-time access to the latest data without delay. By implementing Requester Pays, the survey company can share its valuable data while ensuring that the associated data transfer costs are borne by the European marketing firm accessing the data. This approach aligns with the requirement to keep data transfer costs as low as possible for the survey company.

Sources [1] [Central storage: Amazon S3 as the data lake storage platform – Storage Best Practices for Data and Analytics Applications] (<https://docs.aws.amazon.com/whitepapers/latest/building-data-lakes/amazon-s3-data-lake-storage-platform.html>) [3] [Define storage requirements and transfer data – Semiconductor Design on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/seiconductor-design-on-aws/define-storage-requirements-and-transfer-data.html>) [6] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>)

解析: To minimize data transfer costs for sharing data between the survey company in the United States and the European marketing firm, the best solution is: A. Configure the Requester Pays feature on the company's S3 bucket. Here's an overview of how to implement this solution and why it's the most cost-effective option:

1. Enable Requester Pays on the S3 bucket

- Log in to the AWS Management Console and navigate to the S3 service.

- Select the bucket containing the survey data. - Go to the "Properties" tab. - Scroll down to the "Requester Pays" section and enable it.

2. Configure access permissions

- In the bucket's "Permissions" tab, update the bucket policy to allow the marketing firm's AWS account to access the objects.

- Ensure the principle of least privilege is applied by granting only necessary permissions.

3. Provide access information to the marketing firm

- Share the bucket name and region with the European marketing firm.

- Instruct them on how to access the data using their own AWS credentials.

4. Verify and monitor usage

- Use AWS CloudTrail and S3 server access logging to monitor access to the bucket.

- Regularly review access patterns and costs to ensure the arrangement is working as expected.

This solution is optimal because:

- It keeps the data in a single location, avoiding duplication and synchronization issues.
- The marketing firm pays for the data transfer and request costs, reducing expenses for the survey company.
- It's simple to set up and doesn't require ongoing management of replication or sync processes.
- It allows for real-time access to the latest data without delay.

By implementing Requester Pays, the survey company can share its valuable data while ensuring that the associated data transfer costs are borne by the European marketing firm accessing the data. This approach aligns with the requirement to keep data transfer costs as low as possible for the survey company.

Sources [1] [Central storage: Amazon S3 as the data lake storage platform – Storage Best Practices for Data and Analytics Applications] (<https://docs.aws.amazon.com/whitepapers/latest/building-data-lakes/amazon-s3-data-lake-storage-platform.html>) [3] [Define storage requirements and transfer data – Semiconductor Design on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/semiconductor-design-on-aws/define-storage-requirements-and-transfer-data.html>) [6] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>)

78. Question #89A 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?

- 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.

答案：A

解析：Enabling versioning on the S3 bucket ensures that every version of the documents is kept, allowing the company to recover them in case of accidental deletion. Enabling MFA Delete requires users to provide an MFA code when attempting to delete objects, adding an extra layer of security to prevent accidental deletions. This solution provides a more secure way to handle the audit documents in S3.

解析：Enabling versioning on the S3 bucket ensures that every version of the documents is kept, allowing the company to recover them in case of accidental deletion. Enabling MFA Delete requires users to provide an MFA code when attempting to delete objects, adding an extra layer of security to prevent accidental deletions. This solution provides a more secure way to handle the audit documents in S3.

79. Question #90A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours. The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue. Which solution will meet this requirement with the LEAST operational overhead?

- A. Modify the DB instance to be a Multi-AZ deployment.
- B. Create a read replica of the database. Configure the script to query only the read replica.
- C. Instruct the development team to manually export the entries in the database at the end of each day.
- D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

答案: B

解析: Creating a read replica of the Amazon RDS DB instance allows the script to query the read replica instead of the primary instance. This offloads the read queries from the primary instance, improving its performance for development tasks. The read replica can handle the query load, and since it is asynchronously updated from the primary instance, it does not impact the overall operational overhead significantly.

解析: Creating a read replica of the Amazon RDS DB instance allows the script to query the read replica instead of the primary instance. This offloads the read queries from the primary instance, improving its performance for development tasks. The read replica can handle the query load, and since it is asynchronously updated from the primary instance, it does not impact the overall operational overhead significantly.

80. Question #91A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet. Which solution will meet these requirements?

- A. Configure an S3 gateway endpoint.
- B. Create an S3 bucket in a private subnet.
- C. Create an S3 bucket in the same AWS Region as the EC2 instances.
- D. Configure a NAT gateway in the same subnet as the EC2 instances.

答案: A

解析: An S3 gateway endpoint is a VPC endpoint that allows the EC2 instances to access S3 services without traversing the internet. This solution meets the company's security requirements by ensuring that all

traffic between the EC2 instances and S3 stays within the AWS network, eliminating the need for a NAT gateway or VPN connection.

解析: An S3 gateway endpoint is a VPC endpoint that allows the EC2 instances to access S3 services without traversing the internet. This solution meets the company's security requirements by ensuring that all traffic between the EC2 instances and S3 stays within the AWS network, eliminating the need for a NAT gateway or VPN connection.

81. Question #93A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability. The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes. A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay. Which solution meets these requirements?

- A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
- B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
- D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

答案: B

解析: Using Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production ensures high availability and scalability. To address the

issue of application latency during the export process, the architect should recommend using database cloning. Cloning allows for the creation of a staging database on-demand without impacting the production environment, thus reducing latency and enabling the development team to work with the staging environment without delay.

解析: Using Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production ensures high availability and scalability. To address the issue of application latency during the export process, the architect should recommend using database cloning. Cloning allows for the creation of a staging database on-demand without impacting the production environment, thus reducing latency and enabling the development team to work with the staging environment without delay.

82. Question #94A 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?

- 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.

答案: C

解析: Using AWS Lambda in combination with Amazon S3 and Amazon SQS provides a serverless solution that automatically scales to handle varying upload volumes without requiring any manual intervention. When a file is uploaded to S3, an event notification is sent to an SQS queue, which triggers a Lambda function to process the data. The processed JSON file can then be stored in Amazon DynamoDB. This solution minimizes operational overhead by leveraging the managed and serverless nature of these AWS services.

解析: Using AWS Lambda in combination with Amazon S3 and Amazon SQS provides a serverless solution that automatically scales to handle varying upload volumes without requiring any manual intervention. When a file is uploaded to S3, an event notification is sent to an SQS queue, which triggers a Lambda function to process the data. The processed JSON file can then be stored in Amazon DynamoDB. This solution minimizes operational overhead by leveraging the managed and serverless nature of these AWS services.

83. Question #70A 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?

- 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.

答案: C

解析: Option C is the correct answer because it replaces the NLB with an Application Load Balancer (ALB), which supports HTTP health checks. This allows the ALB to detect HTTP errors and take appropriate actions to replace unhealthy instances, improving the application's availability without the need for custom scripts or code.

解析: Option C is the correct answer because it replaces the NLB with an Application Load Balancer (ALB), which supports HTTP health checks. This allows the ALB to detect HTTP errors and take appropriate actions to replace unhealthy instances, improving the application's availability without the need for custom scripts or code.

84. Question #71A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour. What should the solutions architect recommend to meet these requirements?

- A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
- B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
- C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
- D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

答案: B

解析: Option B is the correct answer because it utilizes DynamoDB point-in-time recovery, which allows for continuous backups and the ability to restore the table to any point in time within the last 35 days. This meets the RPO of 15 minutes as it provides a recent point in time to restore from. Additionally, the recovery process can be completed within the RTO of 1 hour, satisfying both objectives.

解析: Option B is the correct answer because it utilizes DynamoDB point-in-time recovery, which allows for continuous backups and the ability to restore the table to any point in time within the last 35 days. This meets the RPO of 15 minutes as it provides a recent point in time to restore from. Additionally, the recovery process can be completed within the RTO of 1 hour, satisfying both objectives.

85. Question #72A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs. How can the solutions architect meet this requirement?

- A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
- B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.
- C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.
- D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

答案: D

解析: Option D is the correct answer because it involves deploying an S3 VPC gateway endpoint, which allows the application to access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This reduces data transfer fees and improves performance by avoiding public internet routes.

解析: Option D is the correct answer because it involves deploying an S3 VPC gateway endpoint, which allows the application to access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This reduces data transfer fees and improves performance by avoiding public internet routes.

86. Question #75A 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?
- 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.

答案: A

解析: Option A is the correct answer because it leverages AWS Lambda, a serverless compute service, to handle the application layer, allowing for automatic scaling and improved performance without the need for managing infrastructure. Additionally, using Amazon SQS for communication between services decouples them, ensuring that one tier's overload does not cause

transactions to be dropped, and it provides a reliable messaging system. This solution modernizes the application and is operationally efficient.

解析: Option A is the correct answer because it leverages AWS Lambda, a serverless compute service, to handle the application layer, allowing for automatic scaling and improved performance without the need for managing infrastructure. Additionally, using Amazon SQS for communication between services decouples them, ensuring that one tier's overload does not cause transactions to be dropped, and it provides a reliable messaging system. This solution modernizes the application and is operationally efficient.

87. Question #95An 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?

- 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.

答案: D

解析: The solutions architect should recommend option D: Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database. This approach allows the application to offload read traffic from the source database, thus improving its performance. Ensuring that the read replicas have the same compute and storage resources as the source database helps guarantee that they can effectively handle the read workload.

解析: The solutions architect should recommend option D: Create read replicas for the database. Configure the read replicas with the same

compute and storage resources as the source database. This approach allows the application to offload read traffic from the source database, thus improving its performance. Ensuring that the read replicas have the same compute and storage resources as the source database helps guarantee that they can effectively handle the read workload.

88. Question #96 An Amazon EC2 administrator created the following policy associated with an IAM group containing several users: What is the effect of this policy?

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:TerminateInstances",  
            "Resource": "*",  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "10.100.100.0/24"  
                }  
            }  
        },  
        {  
            "Effect": "Deny",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        }  
    ]  
}
```

- 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.

答案: C

解析: The correct answer is C. The policy allows users to terminate an EC2 instance in the us-east-1 Region, but only if their source IP address is 10.100.100.254. This is determined by the IAM Conditions which specify that the action is allowed only if the region is not equal to "us-east-1" and if the source IP is 10.100.100.254.

解析: The correct answer is C. The policy allows users to terminate an EC2 instance in the us-east-1 Region, but only if their source IP address is 10.100.100.254. This is determined by the IAM Conditions which specify that the action is allowed only if the region is not equal to "us-east-1" and if the source IP is 10.100.100.254.

89. Question #97A 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?

- 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.

答案: D

解析: The solution that meets the requirements is D: Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication. Amazon FSx for Windows File Server is designed to provide a fully managed, highly available file storage service that is compatible with Windows Server workloads and can be integrated with an

existing Active Directory, making it the ideal choice for migrating a SharePoint deployment that requires shared file storage and Active Directory integration.

解析: The solution that meets the requirements is D: Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication. Amazon FSx for Windows File Server is designed to provide a fully managed, highly available file storage service that is compatible with Windows Server workloads and can be integrated with an existing Active Directory, making it the ideal choice for migrating a SharePoint deployment that requires shared file storage and Active Directory integration.

90. Question #98An 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?

- 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.

答案: C

解析: The solutions architect should choose option 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. By doing so, the architect ensures that once a message is picked up by the Lambda function, it remains invisible to other consumers until the function has had enough time to process the message and delete it, thus preventing duplicate invocations of the Lambda function and the resulting multiple email messages. This solution has the least operational overhead as it does not require changes to the queue configuration or the function's code.

解析: The solutions architect should choose option 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. By doing so, the architect ensures that once a message is picked up by the Lambda function, it remains invisible to other consumers until the function has had enough time to process the message and delete it, thus preventing duplicate invocations of the Lambda function and the resulting multiple email messages. This solution has the least operational overhead as it does not require changes to the queue configuration or the function's code.

91. Question #99A 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?
- 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.

答案: D

解析: The correct solution is D: Create an Amazon FSx for Lustre file system. Amazon FSx for Lustre is a fully managed service specifically designed for high-performance computing workloads, such as gaming applications, that require the Lustre parallel file system. It provides a high-throughput, low-latency file system that is accessible by Lustre clients, meeting the company's requirements for a fully managed shared storage solution.

解析: The correct solution is D: Create an Amazon FSx for Lustre file system. Amazon FSx for Lustre is a fully managed service specifically designed for high-performance computing workloads, such as gaming applications, that require the Lustre parallel file system. It provides a high-throughput, low-latency file system that is accessible by Lustre clients, meeting the company's requirements for a fully managed shared storage solution.

92. Question #100A 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?

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.

答案：C

解析：The solution that meets the requirements with the least operational overhead is option C: Create an AWS Key Management Service (AWS KMS) customer managed key and store the encrypted data on Amazon S3. AWS KMS provides a secure way to perform encryption operations, and by allowing the EC2 role to use the KMS key, the process is streamlined and does not require manual intervention for each certificate update. Amazon S3 is a highly available storage service that automatically replicates data across multiple availability zones, ensuring the data's durability and availability with minimal configuration and management effort.

解析：The solution that meets the requirements with the least operational overhead is option C: Create an AWS Key Management Service (AWS KMS) customer managed key and store the encrypted data on Amazon S3. AWS KMS provides a secure way to perform encryption operations, and by allowing the EC2 role to use the KMS key, the process is streamlined and does not require manual intervention for each certificate update. Amazon S3 is a highly available storage service that automatically replicates data across multiple availability zones, ensuring the data's durability and availability with minimal configuration and management effort.

93. Question #101A 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?

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.

答案：A

解析：The correct answer is A. NAT gateways are used to allow instances in private subnets to connect to the internet while preventing inbound traffic from the internet from reaching them. By creating a NAT gateway in each public subnet and updating the route tables to use these NAT gateways, the architect ensures that the private subnets can access the internet while maintaining their private isolation. This approach is also scalable and provides high availability across multiple AZs.

解析：The correct answer is A. NAT gateways are used to allow instances in private subnets to connect to the internet while preventing inbound traffic from the internet from reaching them. By creating a NAT gateway in each public subnet and updating the route tables to use these NAT gateways, the architect ensures that the private subnets can access the internet while maintaining their private isolation. This approach is also scalable and provides high availability across multiple AZs.

94. Question #103A 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?
- 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.

答案：A

解析：The correct answer is A. AWS Glue job bookmarks are a feature that allows an ETL job to track the data that has already been processed during a previous run. By using job bookmarks, the architect can ensure that only new data is processed in each subsequent run, which improves efficiency and reduces processing time and costs. Deleting data (Option B) is not necessary and would result in data loss. Changing the NumberOfWorkers (Option C) does not address the issue of reprocessing old data. Using a FindMatches ML transform (Option D) is unrelated to the problem of processing only new data.

解析：The correct answer is A. AWS Glue job bookmarks are a feature that allows an ETL job to track the data that has already been processed during a previous run. By using job bookmarks, the architect can ensure that only new data is processed in each subsequent run, which improves efficiency and reduces processing time and costs. Deleting data (Option B) is not necessary and would result in data loss. Changing the NumberOfWorkers (Option C) does not address the issue of reprocessing old data. Using a FindMatches ML transform (Option D) is unrelated to the problem of processing only new data.

95. Question #105A 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?

- 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.

答案: D

解析: The correct answer is D. The principle of least privilege dictates that the Lambda function should be granted only the permissions necessary to perform its intended task. In this scenario, the function needs to be invoked by Amazon EventBridge. Option D adds a resource-based policy that specifically allows the EventBridge service to invoke the Lambda function. This approach provides the narrowest possible permission set, as it restricts the invoke action to only the EventBridge service, without granting unnecessary permissions to other AWS services or principals.

解析: The correct answer is D. The principle of least privilege dictates that the Lambda function should be granted only the permissions necessary to perform its intended task. In this scenario, the function needs to be invoked by Amazon EventBridge. Option D adds a resource-based policy that specifically allows the EventBridge service to invoke the Lambda function. This approach provides the narrowest possible permission set, as it restricts the invoke action to only the EventBridge service, without granting unnecessary permissions to other AWS services or principals.

96. Question #106A 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?

- 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

答案: D

解析: The correct answer is D. SSE-KMS with automatic rotation provides encryption at rest using keys managed by AWS Key Management Service

(KMS). This option is the most operationally efficient because it automates the key rotation process, ensuring that the encryption keys are updated annually as required for compliance. This automation reduces the administrative burden and the risk of forgetting to manually rotate keys. Additionally, AWS KMS supports logging of key usage via AWS CloudTrail, which aids in auditing and compliance monitoring. SSE-C (Option A) and SSE-S3 (Option B) do not support automatic key rotation or logging of key usage. Manual key rotation (Option C) would require more operational effort and could lead to human error.

解析: The correct answer is D. SSE-KMS with automatic rotation provides encryption at rest using keys managed by AWS Key Management Service (KMS). This option is the most operationally efficient because it automates the key rotation process, ensuring that the encryption keys are updated annually as required for compliance. This automation reduces the administrative burden and the risk of forgetting to manually rotate keys. Additionally, AWS KMS supports logging of key usage via AWS CloudTrail, which aids in auditing and compliance monitoring. SSE-C (Option A) and SSE-S3 (Option B) do not support automatic key rotation or logging of key usage. Manual key rotation (Option C) would require more operational effort and could lead to human error.

97. Question #107A 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?

- 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.

答案: B

解析: Based on the requirements for the bicycle sharing company's multi-tier architecture to track bicycle locations during peak hours, the most viable option is: B. Use Amazon API Gateway with AWS Lambda This solution meets the requirements for the following reasons: 1. REST API accessibility: Amazon API Gateway provides a fully managed service to create, publish, and maintain RESTful APIs. This satisfies the requirement for data points to be accessible via a REST API. 2. Serverless architecture: AWS Lambda allows for serverless compute, which can efficiently handle the processing of location data during peak operating hours without the need to manage infrastructure. 3. Scalability: Both API Gateway and Lambda can automatically scale to handle varying loads, which is crucial during peak operating hours. 4. Integration with existing analytics: Lambda functions can be easily configured to store the location data in a format compatible with the company's existing analytics platform. 5. Real-time processing: This combination allows for real-time processing and storage of location data as it's received. To implement this solution effectively, consider the following best practices: 1. Use API Gateway's request throttling and caching features to manage high traffic during peak hours. 2. Implement appropriate authentication and authorization mechanisms in API Gateway to secure access to the location data. 3. Configure Lambda functions with the principle of least privilege, granting only the necessary permissions to interact with other AWS services. 4. Use AWS X-Ray for tracing and monitoring the performance of your API and Lambda functions. 5. Consider using Amazon DynamoDB or another suitable database service to store the location data for quick retrieval and analysis. 6. Implement error handling and retry mechanisms in your Lambda functions to ensure data reliability. 7. Use AWS CloudWatch for monitoring and setting up alarms for any anomalies in the system. Remember to thoroughly test this architecture in a non-production environment before deploying it to ensure it meets your specific requirements and performance expectations.

Sources [1] [Implementing an analytics strategy for your Amazon selling partner data – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-gen-ai-selling-partner-api/analytics->

capabilities.html) [3] [Introduction – AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda] (<https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/introduction.html>)

解析: Based on the requirements for the bicycle sharing company's multi-tier architecture to track bicycle locations during peak hours, the most viable option is: B. Use Amazon API Gateway with AWS Lambda This solution meets the requirements for the following reasons: 1. REST API accessibility: Amazon API Gateway provides a fully managed service to create, publish, and maintain RESTful APIs. This satisfies the requirement for data points to be accessible via a REST API. 2. Serverless architecture: AWS Lambda allows for serverless compute, which can efficiently handle the processing of location data during peak operating hours without the need to manage infrastructure. 3. Scalability: Both API Gateway and Lambda can automatically scale to handle varying loads, which is crucial during peak operating hours. 4. Integration with existing analytics: Lambda functions can be easily configured to store the location data in a format compatible with the company's existing analytics platform. 5. Real-time processing: This combination allows for real-time processing and storage of location data as it's received. To implement this solution effectively, consider the following best practices: 1. Use API Gateway's request throttling and caching features to manage high traffic during peak hours. 2. Implement appropriate authentication and authorization mechanisms in API Gateway to secure access to the location data. 3. Configure Lambda functions with the principle of least privilege, granting only the necessary permissions to interact with other AWS services. 4. Use AWS X-Ray for tracing and monitoring the performance of your API and Lambda functions. 5. Consider using Amazon DynamoDB or another suitable database service to store the location data for quick retrieval and analysis. 6. Implement error handling and retry mechanisms in your Lambda functions to ensure data reliability. 7. Use AWS CloudWatch for monitoring and setting up alarms for any anomalies in the system. Remember to thoroughly test this architecture in a non-production environment before deploying it to

ensure it meets your specific requirements and performance expectations.

Sources [1] [Implementing an analytics strategy for your Amazon selling partner data – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-gen-ai-selling-partner-api/analytics-capabilities.html>) [3] [Introduction – AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda] (<https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/introduction.html>)

98. Question #108A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems. Which design should a solutions architect recommend?

- A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.
- B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.
- C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.
- D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

答案：A

解析：Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume. This design offers several advantages: 1. Real-time processing: The Lambda function can be triggered immediately when the database is updated, ensuring timely removal of sold

listings from the website. 2. Decoupling: Using SQS as an intermediary between the database update and target systems allows for better scalability and fault tolerance. 3. Flexibility: Multiple target systems can consume messages from the SQS queue independently, allowing for easy addition or removal of target systems without affecting the core process. 4. Efficient resource utilization: Lambda functions are serverless and only run when needed, reducing costs and management overhead. 5. Reliable message delivery: SQS ensures that messages are delivered at least once to the target systems, even if they are temporarily unavailable.

Implementation considerations:

1. Configure the Lambda function with appropriate permissions to access the RDS database and send messages to the SQS queue.
2. Implement error handling and retries in the Lambda function to ensure robustness.
3. Set up appropriate monitoring and alerting using Amazon CloudWatch to track the performance and health of the Lambda function and SQS queue.
4. Consider using SQS dead-letter queues to handle any messages that fail to be processed by the target systems.
5. Implement proper security measures, such as encryption at rest for the SQS queue and in-transit encryption for communication between services.
6. Ensure that the target systems have the necessary permissions to consume messages from the SQS queue.

By following this design and these best practices, you can create a scalable, reliable, and efficient system for updating the website and notifying target systems when automobiles are sold.

Sources [1] [Using AWS Lambda with Amazon RDS – AWS Lambda]

(<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>) [3]

[Welcome – Amazon Relational Database Service]

(<https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/Welcome.html>)

[6] [Tutorial: Using a Lambda function to access an Amazon RDS database – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-lambda-tutorial.html>)

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

1. Real-time processing: The Lambda function can be triggered

immediately when the database is updated, ensuring timely removal of sold listings from the website. 2. Decoupling: Using SQS as an intermediary between the database update and target systems allows for better scalability and fault tolerance. 3. Flexibility: Multiple target systems can consume messages from the SQS queue independently, allowing for easy addition or removal of target systems without affecting the core process. 4. Efficient resource utilization: Lambda functions are serverless and only run when needed, reducing costs and management overhead. 5. Reliable message delivery: SQS ensures that messages are delivered at least once to the target systems, even if they are temporarily unavailable.

Implementation considerations:

1. Configure the Lambda function with appropriate permissions to access the RDS database and send messages to the SQS queue.
2. Implement error handling and retries in the Lambda function to ensure robustness.
3. Set up appropriate monitoring and alerting using Amazon CloudWatch to track the performance and health of the Lambda function and SQS queue.
4. Consider using SQS dead-letter queues to handle any messages that fail to be processed by the target systems.
5. Implement proper security measures, such as encryption at rest for the SQS queue and in-transit encryption for communication between services.
6. Ensure that the target systems have the necessary permissions to consume messages from the SQS queue.

By following this design and these best practices, you can create a scalable, reliable, and efficient system for updating the website and notifying target systems when automobiles are sold.

Sources [1] [Using AWS Lambda with Amazon RDS – AWS Lambda]

(<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>) [3]

[Welcome – Amazon Relational Database Service]

(<https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/Welcome.html>)

[6] [Tutorial: Using a Lambda function to access an Amazon RDS database – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-lambda-tutorial.html>)

99. Question #109A 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?

- A. Create an S3 Glacier vault. Apply a write-once, read-many (WORM) vault lock policy to the objects.
- B. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket's default retention mode for new objects.
- C. Create an S3 bucket. Use AWS CloudTrail to track any S3 API events that modify the objects. Upon notification, restore the modified objects from any backup versions that the company has.
- D. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

答案: D

解析: The solution that meets the requirements is Option D. By enabling S3 Object Lock and adding a legal hold to the objects, the data becomes immutable for a nonspecific amount of time. Only users with the appropriate IAM permissions can remove the legal hold and delete the objects. This ensures that the data is protected against unauthorized changes and deletions, while still allowing specific users to perform these actions when necessary.

解析: The solution that meets the requirements is Option D. By enabling S3 Object Lock and adding a legal hold to the objects, the data becomes immutable for a nonspecific amount of time. Only users with the appropriate IAM permissions can remove the legal hold and delete the objects. This ensures that the data is protected against unauthorized changes and deletions, while still allowing specific users to perform these actions when necessary.

100. Question #111A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application

running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity. Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
- D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

答案: D

解析: The architecture that offers the highest availability is Option D. This option includes the use of Amazon MQ with active/standby brokers across two Availability Zones, which ensures high availability for the message queue. Additionally, using an Auto Scaling group for the consumer EC2 instances provides scalability and fault tolerance, as it can automatically replace unhealthy instances. Lastly, using Amazon RDS for MySQL with Multi-AZ deployment ensures that the database layer is also highly available, reducing the risk of downtime.

解析: The architecture that offers the highest availability is Option D. This option includes the use of Amazon MQ with active/standby brokers across two Availability Zones, which ensures high availability for the message queue. Additionally, using an Auto Scaling group for the consumer EC2 instances provides scalability and fault tolerance, as it can automatically replace unhealthy instances. Lastly, using Amazon RDS for MySQL with Multi-AZ deployment ensures that the database layer is also

highly available, reducing the risk of downtime.

101. Question #112A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
- B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests.
- C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.
- D. Use a high performance computing (HPC) solution such as AWS ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

答案：A

解析：The solution that meets the requirements with the least operational overhead is Option A. AWS Fargate is a serverless compute engine for containers that removes the need to provision and manage servers, which greatly reduces operational overhead. By using Fargate with Amazon ECS and an Application Load Balancer, the company can easily scale the application to handle the increased load without significant code changes or development effort.

解析：The solution that meets the requirements with the least operational overhead is Option A. AWS Fargate is a serverless compute engine for containers that removes the need to provision and manage servers, which greatly reduces operational overhead. By using Fargate with Amazon ECS and an Application Load Balancer, the company can easily scale the

application to handle the increased load without significant code changes or development effort.

102. Question #113A 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?

- 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.

答案: C

解析: The solution that meets the requirements with the least operational overhead is Option C. Using an AWS Snowball Edge Storage Optimized device allows for the transfer of large amounts of data into and out of AWS with minimal network bandwidth requirements. Additionally, by creating a custom transformation job using AWS Glue, the company can continue to run the transformation job in the AWS Cloud without the need to pause the application, as AWS Glue is a serverless data integration service that can handle extract, transform, and load (ETL) tasks.

解析: The solution that meets the requirements with the least operational overhead is Option C. Using an AWS Snowball Edge Storage Optimized device allows for the transfer of large amounts of data into and out of AWS with

minimal network bandwidth requirements. Additionally, by creating a custom transformation job using AWS Glue, the company can continue to run the transformation job in the AWS Cloud without the need to pause the application, as AWS Glue is a serverless data integration service that can handle extract, transform, and load (ETL) tasks.

103. Question #114A 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 meets these requirements?

- 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.

答案: C

解析: The solution that best meets the requirements is Option C. Using AWS Lambda to process the photos allows for automatic scaling based on the number of photos that need processing. Storing the photos in Amazon S3 provides a highly durable and scalable object storage service that can handle large amounts of data and high traffic. Retaining DynamoDB for metadata storage is efficient because metadata is typically smaller in size and benefits from the fast retrieval times of a NoSQL database like DynamoDB.

解析: The solution that best meets the requirements is Option C. Using AWS Lambda to process the photos allows for automatic scaling based on the number of photos that need processing. Storing the photos in Amazon S3 provides a highly durable and scalable object storage service that can handle large amounts of data and high traffic. Retaining DynamoDB for metadata storage is efficient because metadata is typically smaller in size and benefits from the fast retrieval times of a NoSQL database like DynamoDB.

104. Question #115A 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?

- 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.

答案: C

解析: To meet the requirement of transferring files over a private route without using the internet, the solutions architect should recommend moving the EC2 instances to private subnets (Option C). By creating a VPC endpoint for Amazon S3 and linking it to the route table for the private subnets, the EC2 instances can access S3 directly over the AWS network, ensuring that the data transfer does not leave the AWS environment. This

approach maintains security and complies with the new requirement.

解析: To meet the requirement of transferring files over a private route without using the internet, the solutions architect should recommend moving the EC2 instances to private subnets (Option C). By creating a VPC endpoint for Amazon S3 and linking it to the route table for the private subnets, the EC2 instances can access S3 directly over the AWS network, ensuring that the data transfer does not leave the AWS environment. This approach maintains security and complies with the new requirement.

105. Question #117A 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?

- 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).

答案: A

解析: The solution that meets the requirement with the least operational overhead is Option A. Configuring a CloudWatch Logs subscription to stream logs directly to Amazon OpenSearch Service is a straightforward process that requires minimal setup and maintenance. This approach allows for near-real-time log data transfer to the target service without the need for additional services or custom code.

解析: The solution that meets the requirement with the least operational overhead is Option A. Configuring a CloudWatch Logs subscription to stream logs directly to Amazon OpenSearch Service is a straightforward process that requires minimal setup and maintenance. This approach allows for near-real-time log data transfer to the target service without the need for additional services or custom code.

106. Question #118A 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?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- D. Amazon S3

答案: D

解析: The most cost-effective storage solution for this scenario is Amazon S3 (Option D). Amazon S3 is designed to scale automatically and can handle large amounts of data, making it suitable for storing a 900 TB repository of text documents. It also offers a highly durable storage option with a simple web services interface, allowing for easy integration with Amazon EC2 instances. Moreover, Amazon S3 provides a cost-effective storage option compared to the other services listed, especially for such a large volume of data.

解析: The most cost-effective storage solution for this scenario is Amazon S3 (Option D). Amazon S3 is designed to scale automatically and can handle large amounts of data, making it suitable for storing a 900 TB repository of text documents. It also offers a highly durable storage option with a simple web services interface, allowing for easy

integration with Amazon EC2 instances. Moreover, Amazon S3 provides a cost-effective storage option compared to the other services listed, especially for such a large volume of data.

107. Question #119A 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?
- 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 both 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.

答案：B

解析：The solution that requires the least amount of administrative effort is Option B, setting up AWS Firewall Manager in both Regions and centrally configuring AWS WAF rules. AWS Firewall Manager allows for the centralized management of security rules across multiple accounts and regions, which simplifies the process of protecting resources. By using Firewall Manager, the solutions architect can apply AWS WAF rules consistently across the REST APIs in both specified regions, reducing the administrative overhead.

解析：The solution that requires the least amount of administrative effort is Option B, setting up AWS Firewall Manager in both Regions and centrally configuring AWS WAF rules. AWS Firewall Manager allows for the centralized management of security rules across multiple accounts and regions, which simplifies the process of protecting resources. By using Firewall Manager, the solutions architect can apply AWS WAF rules consistently across the REST APIs in both specified regions, reducing the

administrative overhead.

108. Question #120A 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?

- 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.

答案: B

解析: The correct answer is B. A standard accelerator in AWS Global Accelerator can be used to route traffic to the optimal regional endpoint based on health, client location, and configured policies. This would increase the availability of the company's DNS solution by directing traffic over the AWS global network to the nearest region to the client.

解析: The correct answer is B. A standard accelerator in AWS Global Accelerator can be used to route traffic to the optimal regional endpoint based on health, client location, and configured policies. This would increase the availability of the company's DNS solution by directing

traffic over the AWS global network to the nearest region to the client.

109. Question #121A 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?

- 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).

答案：A

解析：The correct answer is A. According to AWS documentation, you can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance.

解析：The correct answer is A. According to AWS documentation, you can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance.

110. Question #122A 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?

- 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.

答案：B

解析：The correct answer is B. AWS KMS is a fully managed service that makes it easy to create and manage encryption keys. It allows developers to easily encrypt and decrypt data in their applications, and it automatically handles the underlying key management tasks, such as key generation, key rotation, and key deletion, which helps to reduce the operational burden.

解析：The correct answer is B. AWS KMS is a fully managed service that makes it easy to create and manage encryption keys. It allows developers to easily encrypt and decrypt data in their applications, and it automatically handles the underlying key management tasks, such as key generation, key rotation, and key deletion, which helps to reduce the operational burden.

111. Question #123A 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?

- 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.

答案: D

解析: The correct answer is D. By importing the SSL certificate into AWS Certificate Manager (ACM) and creating an Application Load Balancer (ALB) with an HTTPS listener that uses the SSL certificate from ACM, the ALB can offload the SSL termination process from the EC2 instances. This allows the EC2 instances to focus on running the web application, which can help to increase the application's performance.

解析: The correct answer is D. By importing the SSL certificate into AWS Certificate Manager (ACM) and creating an Application Load Balancer (ALB) with an HTTPS listener that uses the SSL certificate from ACM, the ALB can offload the SSL termination process from the EC2 instances. This allows the EC2 instances to focus on running the web application, which can help to increase the application's performance.

112. Question #124A 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?

- A. Implement EC2 Spot Instances.
- B. Purchase EC2 Reserved Instances.
- C. Implement EC2 On-Demand Instances.
- D. Implement the processing on AWS Lambda.

答案: A

解析: The correct answer is A. EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless and can be started and stopped at any time, EC2 Spot Instances would be a good fit for this workload.

解析: The correct answer is A. EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless and can be started and stopped at any time, EC2 Spot Instances would be a good fit for this workload.

113. Question #126A 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?

- 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.

答案: B

解析: The correct answer is B. According to the requirements, data from the most recent 2 years must be highly available and immediately retrievable, which suggests that it should remain in the S3 Standard storage class. After 2 years, the data can be transitioned to S3 Glacier Deep Archive for long-term storage, which is a cost-effective solution for data that is accessed less frequently.

解析: The correct answer is B. According to the requirements, data from the most recent 2 years must be highly available and immediately retrievable, which suggests that it should remain in the S3 Standard storage class. After 2 years, the data can be transitioned to S3 Glacier Deep Archive for long-term storage, which is a cost-effective solution for data that is accessed less frequently.

114. Question #127A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore. Which set of services should a solutions architect recommend to meet these requirements?

- A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

答案: A

解析: Based on the media company's requirements, I recommend the following set of AWS services to meet their storage needs: A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage. Here's a breakdown of how these services address the company's specific requirements: 1. For video processing (10 TB with maximum I/O performance):

- Amazon EBS (Elastic Block Store) is ideal for this use case. It provides high-performance block-level storage that can be attached to Amazon EC2 instances, making it perfect for I/O-intensive workloads like video processing.
- EBS volumes can be provisioned with different performance characteristics to meet the specific needs of video processing tasks.

2. For storing media content

(300 TB of very durable storage): – Amazon S3 (Simple Storage Service) is the best choice for this requirement. It offers industry-leading durability, scalability, and availability for object storage. – S3 is designed for 99.99999999% (11 9's) of durability, making it extremely reliable for storing important media content. – It also provides various storage classes to optimize costs based on access patterns.

3. For archival media storage (900 TB): – Amazon S3 Glacier is the most cost-effective solution for long-term archival storage of infrequently accessed data. – It offers multiple retrieval options to balance cost and access time based on the company's needs. This combination of services provides a comprehensive storage solution that addresses the media company's diverse requirements while optimizing for performance, durability, and cost-effectiveness. Best practices and additional considerations:

1. Implement appropriate data lifecycle policies in S3 to automatically transition less frequently accessed data to lower-cost storage tiers or Glacier.
2. Use AWS Identity and Access Management (IAM) to manage access to these storage services securely.
3. Enable encryption at rest for sensitive data stored in EBS, S3, and Glacier.
4. Regularly backup critical data and test restoration processes.
5. Monitor storage usage and performance using Amazon CloudWatch to optimize costs and performance.
6. Consider using S3 Transfer Acceleration for faster uploads of large media files to S3 from distant geographic locations.
7. Explore using AWS DataSync for efficient data transfer between on-premises storage and AWS storage services during the migration process. Remember to consult the official AWS documentation for the most up-to-date information on these services, their features, and best practices for implementation.

Sources [1] [Choosing an AWS storage service – Choosing an AWS storage service] (<https://docs.aws.amazon.com/decision-guides/latest/storage-on-aws-how-to-choose/choosing-aws-storage-service.html>) [3] [SAA-C03 question | AWS re:Post] (<https://repost.aws/questions/QUHCySI6otStqGft0FHhHe0Q/saa-c03-question>) [6] [Enhance your Migration Evaluator business case using Storage Insights and a Storage Assessment | Migration & Modernization] (<https://aws.amazon.com/blogs/migration-and-modernization/enhance-your-migration-ev>

[valuator-business-case-using-storage-insights-and-a-storage-assessment/](#)

解析: Based on the media company's requirements, I recommend the following set of AWS services to meet their storage needs:

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

Here's a breakdown of how these services address the company's specific requirements:

1. For video processing (10 TB with maximum I/O performance):
 - Amazon EBS (Elastic Block Store) is ideal for this use case. It provides high-performance block-level storage that can be attached to Amazon EC2 instances, making it perfect for I/O-intensive workloads like video processing.
 - EBS volumes can be provisioned with different performance characteristics to meet the specific needs of video processing tasks.
2. For storing media content (300 TB of very durable storage):
 - Amazon S3 (Simple Storage Service) is the best choice for this requirement. It offers industry-leading durability, scalability, and availability for object storage.
 - S3 is designed for 99.99999999% (11 9's) of durability, making it extremely reliable for storing important media content.
 - It also provides various storage classes to optimize costs based on access patterns.
3. For archival media storage (900 TB):
 - Amazon S3 Glacier is the most cost-effective solution for long-term archival storage of infrequently accessed data.
 - It offers multiple retrieval options to balance cost and access time based on the company's needs.
 - This combination of services provides a comprehensive storage solution that addresses the media company's diverse requirements while optimizing for performance, durability, and cost-effectiveness.

Best practices and additional considerations:

1. Implement appropriate data lifecycle policies in S3 to automatically transition less frequently accessed data to lower-cost storage tiers or Glacier.
2. Use AWS Identity and Access Management (IAM) to manage access to these storage services securely.
3. Enable encryption at rest for sensitive data stored in EBS, S3, and Glacier.
4. Regularly backup critical data and test restoration processes.
5. Monitor storage usage and performance using Amazon CloudWatch to optimize costs and performance.
6. Consider using S3 Transfer Acceleration for faster uploads of large media files to S3 from distant geographic locations.
- 7.

Explore using AWS DataSync for efficient data transfer between on-premises storage and AWS storage services during the migration process. Remember to consult the official AWS documentation for the most up-to-date information on these services, their features, and best practices for implementation. Sources [1] [Choosing an AWS storage service – Choosing an AWS storage service] (<https://docs.aws.amazon.com/decision-guides/latest/storage-on-aws-how-to-choose/choosing-aws-storage-service.html>) [3] [SAA-C03 question | AWS re:Post] (<https://repost.aws/questions/QUHCySI6otStqGft0FHhHe0Q/saa-c03-question>) [6] [Enhance your Migration Evaluator business case using Storage Insights and a Storage Assessment | Migration & Modernization] (<https://aws.amazon.com/blogs/migration-and-modernization/enhance-your-migration-evaluator-business-case-using-storage-insights-and-a-storage-assessment/>)

115. Question #128A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead. What should a solutions architect do to meet these requirements?
- A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
 - B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
 - C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
 - D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

答案: B

解析: The correct answer is B. Using Spot Instances in an Amazon EKS managed node group can help minimize cost as Spot Instances are typically less expensive than On-Demand Instances. Amazon EKS is a fully managed service that simplifies the management of Kubernetes clusters, which can help reduce operational overhead.

解析: The correct answer is B. Using Spot Instances in an Amazon EKS managed node group can help minimize cost as Spot Instances are typically less expensive than On-Demand Instances. Amazon EKS is a fully managed service that simplifies the management of Kubernetes clusters, which can help reduce operational overhead.

116. Question #130An 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?

- 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 to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

答案: B

解析: The correct answer is B. A target tracking policy can be used to automatically adjust the desired capacity of the Auto Scaling group based on a specific target value for a metric, in this case, CPU utilization. This ensures that the application maintains the desired performance as demand changes.

解析: The correct answer is B. A target tracking policy can be used to automatically adjust the desired capacity of the Auto Scaling group based on a specific target value for a metric, in this case, CPU utilization. This ensures that the application maintains the desired performance as demand changes.

117. Question #131A 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?

- 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.

答案: D

解析: The correct answer is D. By creating an origin access identity (OAI) and assigning it to the CloudFront distribution, while configuring the S3 bucket so that only the OAI has read permission, the architect can ensure that files are not directly accessible via the S3 URL but are served through CloudFront.

解析: The correct answer is D. By creating an origin access identity (OAI) and assigning it to the CloudFront distribution, while configuring the S3 bucket so that only the OAI has read permission, the architect can ensure that files are not directly accessible via the S3 URL but are served through CloudFront.

118. Question #132A 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?

- 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

答案: A

解析: The correct answer is A. Amazon CloudFront is a content delivery network (CDN) that can distribute content globally with low latency. Amazon S3 can store the historical performance reports, which are then served through CloudFront to ensure a scalable, cost-effective solution with the fastest response times.

解析: The correct answer is A. Amazon CloudFront is a content delivery network (CDN) that can distribute content globally with low latency. Amazon S3 can store the historical performance reports, which are then served through CloudFront to ensure a scalable, cost-effective solution with the fastest response times.

119. Question #133A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system. Which solution will meet these requirements?

- A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
- B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
- C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.
- D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

答案: C

解析: The correct answer is C. Amazon RDS Custom for Oracle allows the company to maintain access to the database's underlying operating system. Additionally, creating a read replica in another AWS Region provides a

disaster recovery solution with minimal operational overhead.

解析: The correct answer is C. Amazon RDS Custom for Oracle allows the company to maintain access to the database's underlying operating system. Additionally, creating a read replica in another AWS Region provides a disaster recovery solution with minimal operational overhead.

120. Question #134A 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?

- 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 keys (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.

答案: C

解析: The correct answer is C. By using the existing S3 bucket and enabling S3 Cross-Region Replication (CRR) along with server-side encryption with Amazon S3 managed encryption keys (SSE-S3), the company can meet the requirements with less operational overhead compared to creating a new S3 bucket. Amazon Athena can then be used to query the

encrypted data.

解析: The correct answer is C. By using the existing S3 bucket and enabling S3 Cross-Region Replication (CRR) along with server-side encryption with Amazon S3 managed encryption keys (SSE-S3), the company can meet the requirements with less operational overhead compared to creating a new S3 bucket. Amazon Athena can then be used to query the encrypted data.

121. Question #135A 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 meet these requirements?

- 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 VPC. Update 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.

答案: D

解析: The correct answer is D. By asking the provider to create a VPC endpoint for the target service and using AWS PrivateLink, the company can establish a private connection that is restricted to the target service. This ensures that the connection is secure and initiated only from the company's VPC.

解析: The correct answer is D. By asking the provider to create a VPC endpoint for the target service and using AWS PrivateLink, the company can establish a private connection that is restricted to the target service. This ensures that the connection is secure and initiated only from the company's VPC.

122. Question #137A 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?

- 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.
- 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.

答案: B

解析: The correct answer is B. By configuring the AWS account root user email addresses as distribution lists that go to a few administrators, the company can ensure that notifications are not missed and are limited to account administrators who can respond to alerts.

解析: The correct answer is B. By configuring the AWS account root user email addresses as distribution lists that go to a few administrators, the company can ensure that notifications are not missed and are limited to account administrators who can respond to alerts.

123. Question #138A company runs its ecommerce application on AWS. Every new order is published as a message 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?

- 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.

答案：B

解析：The correct answer is B. By migrating the queue to Amazon MQ, the company can take advantage of the high availability and failover capabilities of the service. Creating a Multi-AZ Auto Scaling group for the application EC2 instances ensures that the application is available even if one Availability Zone goes down. Migrating the database to Amazon RDS for PostgreSQL with Multi-AZ deployment provides a managed database service with built-in high availability and automatic failover.

解析：The correct answer is B. By migrating the queue to Amazon MQ, the company can take advantage of the high availability and failover capabilities of the service. Creating a Multi-AZ Auto Scaling group for the application EC2 instances ensures that the application is available even if one Availability Zone goes down. Migrating the database to Amazon RDS for PostgreSQL with Multi-AZ deployment provides a managed database service with built-in high availability and automatic failover.

124. Question #139A 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 to the 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?

- 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.

答案: D

解析: The correct answer is D. By configuring S3 replication between the buckets, files are automatically copied to the analysis S3 bucket when they are added to the initial bucket. Setting up event notifications to

trigger Lambda functions and SageMaker Pipelines through Amazon EventBridge provides a serverless way to run pattern-matching code and process the data files with minimal operational overhead.

解析: The correct answer is D. By configuring S3 replication between the buckets, files are automatically copied to the analysis S3 bucket when they are added to the initial bucket. Setting up event notifications to trigger Lambda functions and SageMaker Pipelines through Amazon EventBridge provides a serverless way to run pattern-matching code and process the data files with minimal operational overhead.

125. Question #141A 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 a mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible. How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

- A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
- B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
- C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
- D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

答案: A

解析: The correct answer is A. Deploying the application stack in a single AWS Region and using Amazon CloudFront with the ALB as an origin

can help reduce latency by caching content at edge locations closer to users across the globe. CloudFront can effectively serve both static and dynamic content with low latency.

解析: The correct answer is A. Deploying the application stack in a single AWS Region and using Amazon CloudFront with the ALB as an origin can help reduce latency by caching content at edge locations closer to users across the globe. CloudFront can effectively serve both static and dynamic content with low latency.

126. Question #142A 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?

- 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.

答案: C

解析: The correct answer is C. AWS Global Accelerator is designed to improve performance for applications over UDP by routing traffic to the nearest edge location and providing static IP addresses. It is the appropriate service to use for a gaming application that requires low latency and UDP support. Network Load Balancer is suitable for handling

the UDP traffic, and EC2 Auto Scaling ensures that the application tier is highly available.

解析: The correct answer is C. AWS Global Accelerator is designed to improve performance for applications over UDP by routing traffic to the nearest edge location and providing static IP addresses. It is the appropriate service to use for a gaming application that requires low latency and UDP support. Network Load Balancer is suitable for handling the UDP traffic, and EC2 Auto Scaling ensures that the application tier is highly available.

127. Question #143A 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?

- 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.

答案: D

解析: The correct answer is D. Amazon ECS is a fully managed container orchestration service that allows you to run and scale containerized applications. By containerizing the monolithic application and hosting it on ECS, the company can break it into smaller, more manageable applications. An Application Load Balancer can be used in conjunction with ECS to distribute traffic to the containerized applications, providing a scalable and highly available solution.

解析: The correct answer is D. Amazon ECS is a fully managed container orchestration service that allows you to run and scale containerized applications. By containerizing the monolithic application and hosting it on ECS, the company can break it into smaller, more manageable applications. An Application Load Balancer can be used in conjunction with ECS to distribute traffic to the containerized applications, providing a scalable and highly available solution.

128. Question #144A 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 CPUUtilization metrics are spiking when monthly reports run. What is the MOST cost-effective solution?

- 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.

答案: B

解析: The correct answer is B. Migrating the monthly reporting to an Aurora Replica can offload read traffic from the primary database, which can help reduce the ReadIOPS and CPUUtilization spikes. An Aurora Replica is a cost-effective solution as it allows the primary database to maintain performance while handling the additional read load from reporting.

解析: The correct answer is B. Migrating the monthly reporting to an Aurora Replica can offload read traffic from the primary database, which can help reduce the ReadIOPS and CPUUtilization spikes. An Aurora Replica is a cost-effective solution as it allows the primary database to maintain performance while handling the additional read load from reporting.

129. Question #145A 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?

- 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.

答案: D

解析: The correct answer is D. Migrating the database to Amazon Aurora MySQL can improve performance and scalability. Creating an AMI and using it with a launch template for an Auto Scaling group allows the application to scale seamlessly. Utilizing a Spot Fleet can provide cost savings, and attaching an Application Load Balancer ensures that the load is distributed across available EC2 instances.

解析: The correct answer is D. Migrating the database to Amazon Aurora MySQL can improve performance and scalability. Creating an AMI and using it with a launch template for an Auto Scaling group allows the application to scale seamlessly. Utilizing a Spot Fleet can provide cost

savings, and attaching an Application Load Balancer ensures that the load is distributed across available EC2 instances.

130. Question #146A 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?

- 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.

答案: B

解析: The correct answer is B. Using Reserved Instances for the baseline level of usage can provide cost savings over On-Demand pricing for the steady state workload. Spot Instances can be used for additional capacity during peak hours, leveraging the lower costs of Spot Instances while maintaining the availability of the application.

解析: The correct answer is B. Using Reserved Instances for the baseline level of usage can provide cost savings over On-Demand pricing for the steady state workload. Spot Instances can be used for additional capacity during peak hours, leveraging the lower costs of Spot Instances while maintaining the availability of the application.

131. Question #147A 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?

- 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.

答案：B

解析：The correct answer is B. Storing logs in Amazon S3 and using S3 Lifecycle policies to move older logs to S3 Glacier Deep Archive provides a cost-effective solution for long-term storage of infrequently accessed data. S3 Glacier Deep Archive is designed for archiving data with long retention needs, making it a suitable choice for storing logs for 10 years.

解析：The correct answer is B. Storing logs in Amazon S3 and using S3 Lifecycle policies to move older logs to S3 Glacier Deep Archive provides a cost-effective solution for long-term storage of infrequently accessed data. S3 Glacier Deep Archive is designed for archiving data with long retention needs, making it a suitable choice for storing logs for 10 years.

132. Question #148A company has a data ingestion workflow that includes the following components: An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries, an AWS Lambda function that processes and stores the data. The ingestion workflow occasionally fails because of network connectivity issues. When failure occurs, the corresponding data is not ingested unless the company manually reruns the job. What should a solutions architect do to ensure that all notifications are eventually processed?

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

- B. Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.
- C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries.
- D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue.

答案: D

解析: The correct answer is D. By configuring an Amazon SQS queue as the on-failure destination for the SNS topic, the Lambda function can process messages from the queue, ensuring that all notifications are eventually processed even if there are temporary network connectivity issues.

解析: The correct answer is D. By configuring an Amazon SQS queue as the on-failure destination for the SNS topic, the Lambda function can process messages from the queue, ensuring that all notifications are eventually processed even if there are temporary network connectivity issues.

133. Question #149A 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?

- 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.

答案：A

解析：The correct answer is A. Using an Amazon SQS FIFO (First-In-First-Out) queue ensures that the order of messages is maintained, which is critical for processing event data in the specific order it was received. AWS Lambda can be triggered to process messages from the FIFO queue, providing a serverless solution that minimizes operational overhead.

解析：The correct answer is A. Using an Amazon SQS FIFO (First-In-First-Out) queue ensures that the order of messages is maintained, which is critical for processing event data in the specific order it was received. AWS Lambda can be triggered to process messages from the FIFO queue, providing a serverless solution that minimizes operational overhead.

134. Question #150A 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?

- 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.

答案：A

解析：The correct answer is A. Creating Amazon CloudWatch composite alarms allows the architect to combine multiple metric alarms into a single alarm that triggers only when all conditions are met, such as high

CPU utilization and high read IOPS. This approach reduces false alarms by ensuring that the alarm is only triggered when both conditions occur simultaneously.

解析: The correct answer is A. Creating Amazon CloudWatch composite alarms allows the architect to combine multiple metric alarms into a single alarm that triggers only when all conditions are met, such as high CPU utilization and high read IOPS. This approach reduces false alarms by ensuring that the alarm is only triggered when both conditions occur simultaneously.

135. Question #152A 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?

- 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.

答案: D

解析: The correct answer is D. Creating AWS Lambda functions to manage the start and stop of the Amazon RDS DB instance based on a predefined schedule can minimize costs by only running the DB instance during the hours it is needed. Amazon EventBridge can trigger these Lambda functions at the specified times, ensuring that the DB instance is not running and

incurring costs when not in use.

解析: The correct answer is D. Creating AWS Lambda functions to manage the start and stop of the Amazon RDS DB instance based on a predefined schedule can minimize costs by only running the DB instance during the hours it is needed. Amazon EventBridge can trigger these Lambda functions at the specified times, ensuring that the DB instance is not running and incurring costs when not in use.

136. Question #153A 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?

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

答案: D

解析: The correct answer is D. Implementing an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days is a cost-effective solution. This allows the company to maintain fast access to frequently downloaded ringtones while moving less frequently accessed files to a lower-cost storage tier.

解析: The correct answer is D. Implementing an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days is a cost-effective solution. This allows the company to maintain fast access to frequently downloaded ringtones while moving less frequently accessed files to a lower-cost storage tier.

137. Question #154A 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?

- 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.

答案: B

解析: The correct answer is B. Using S3 Object Lock in compliance mode with a retention period of 365 days will prevent any user, including the root user, from deleting or modifying the objects within the S3 bucket for the duration of the retention period. This meets the requirement to keep files for at least 1 year without the ability to modify or delete them.

解析: The correct answer is B. Using S3 Object Lock in compliance mode with a retention period of 365 days will prevent any user, including the root user, from deleting or modifying the objects within the S3 bucket for the duration of the retention period. This meets the requirement to keep files for at least 1 year without the ability to modify or delete them.

138. Question #155A 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?

- 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.

答案：C

解析：The correct answer is C. Deploying Amazon CloudFront and connecting it to the S3 buckets will cache the media files at edge locations around the world. This ensures that users can access the content quickly and reliably, no matter their geographical location.

解析：The correct answer is C. Deploying Amazon CloudFront and connecting it to the S3 buckets will cache the media files at edge locations around the world. This ensures that users can access the content quickly and reliably, no matter their geographical location.

139. Question #158A 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?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

答案：A

解析：The correct answer is A. Amazon CloudFront is a content delivery network (CDN) that can be used to distribute live and on-demand streaming content globally. It caches content at edge locations close to viewers, reducing latency and improving the streaming experience for a global

audience.

解析: The correct answer is A. Amazon CloudFront is a content delivery network (CDN) that can be used to distribute live and on-demand streaming content globally. It caches content at edge locations close to viewers, reducing latency and improving the streaming experience for a global audience.

140. Question #160An 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?

- A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- B. Amazon S3 Glacier
- C. Amazon S3 Standard
- D. Amazon RDS for PostgreSQL

答案: C

解析: The correct answer is C. Amazon S3 Standard is a highly durable storage option that provides fast, immediate access to stored data, which is suitable for the company's requirement for millisecond-level access. It is also a cost-effective solution for storing data that needs to be retained for 30 days.

解析: The correct answer is C. Amazon S3 Standard is a highly durable storage option that provides fast, immediate access to stored data, which is suitable for the company's requirement for millisecond-level access. It is also a cost-effective solution for storing data that needs to be retained for 30 days.

141. Question #161A 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?

- 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.

答案: B

解析: The correct answer is B. AWS Lambda can run the Python code in response to new JSON documents added to an S3 bucket, providing a serverless solution that scales automatically with the number of documents. Storing the results in an Amazon Aurora DB cluster ensures high availability and durability for the processed data.

解析: The correct answer is B. AWS Lambda can run the Python code in response to new JSON documents added to an S3 bucket, providing a serverless solution that scales automatically with the number of documents. Storing the results in an Amazon Aurora DB cluster ensures high availability and durability for the processed data.

142. Question #162A 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 workload 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?

- 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

答案：A

解析：The correct answer is A. Amazon FSx for Lustre is a high-performance file system that is designed for HPC workloads and can be integrated with Amazon S3 for long-term storage. This combination provides the performance needed for HPC applications while also offering persistent storage for output data.

解析：The correct answer is A. Amazon FSx for Lustre is a high-performance file system that is designed for HPC workloads and can be integrated with Amazon S3 for long-term storage. This combination provides the performance needed for HPC applications while also offering persistent storage for output data.

143. Question #163A 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?

- 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.

答案：A

解析：The correct answer is A. Using Amazon ECS with the AWS Fargate launch type provides a serverless container management service that eliminates the need to manage the underlying EC2 instances. This minimizes operational overhead and, combined with target tracking, allows for automatic scaling based on demand.

解析：The correct answer is A. Using Amazon ECS with the AWS Fargate launch type provides a serverless container management service that eliminates the need to manage the underlying EC2 instances. This minimizes operational overhead and, combined with target tracking, allows for automatic scaling based on demand.

144. Question #164A 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?

- 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.

答案: C

解析: The correct answer is C. Amazon SQS provides a managed message queuing service that can handle the buffering of messages, with the ability to configure dead-letter queues for messages that cannot be processed successfully. This ensures that messages are not lost and can be retried or analyzed for failure reasons without impacting the processing of other messages.

解析: The correct answer is C. Amazon SQS provides a managed message queuing service that can handle the buffering of messages, with the ability to configure dead-letter queues for messages that cannot be processed successfully. This ensures that messages are not lost and can be retried or analyzed for failure reasons without impacting the processing of other messages.

145. Question #165A 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?

- 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.

答案: D

解析: The correct answer is D. By configuring an origin access identity (OAI) for the S3 bucket, the architect can restrict access to the S3 bucket so that only CloudFront can access the content. Additionally, enabling AWS WAF on the CloudFront distribution allows for the inspection of all incoming requests to the website, complying with the company's security policy.

解析: The correct answer is D. By configuring an origin access identity (OAI) for the S3 bucket, the architect can restrict access to the S3 bucket so that only CloudFront can access the content. Additionally, enabling AWS WAF on the CloudFront distribution allows for the inspection of all incoming requests to the website, complying with the company's security policy.

146. Question #1660
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?

- 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.

答案: D

解析: The correct answer is D. Amazon CloudFront is a content delivery network (CDN) that can distribute the static HTML pages globally. By

using CloudFront with the S3 bucket as its origin, the architect can ensure that the pages are served to users from edge locations closest to them, reducing latency and handling the high volume of traffic efficiently.

解析: The correct answer is D. Amazon CloudFront is a content delivery network (CDN) that can distribute the static HTML pages globally. By using CloudFront with the S3 bucket as its origin, the architect can ensure that the pages are served to users from edge locations closest to them, reducing latency and handling the high volume of traffic efficiently.

147. Question #167A 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?

- 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.

答案: C

解析: Based on the requirements for the company's production application running on Amazon EC2 instances, processing messages from an Amazon SQS queue with unpredictable and intermittent traffic, the most cost-effective solution that meets these requirements is: C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity. Here's why this solution is the most cost-effective while meeting the requirements: 1. Cost-effectiveness: – Reserved Instances provide significant discounts compared to On-Demand pricing for

a committed baseline capacity. – Spot Instances offer up to 90% cost savings compared to On-Demand instances for handling variable workloads.

2. Handling unpredictable and intermittent traffic: – Reserved Instances cover the baseline capacity, ensuring a minimum level of resources is always available. – Spot Instances can be used to scale up during traffic spikes, providing additional capacity when needed.

3. Continuous processing without downtime: – Reserved Instances provide a stable base for continuous processing. – By using a mix of instance types and spreading across multiple Availability Zones, the risk of Spot Instance interruptions can be mitigated.

4. Flexibility: – This hybrid approach allows for adjusting the balance between cost savings and stability based on the application's specific needs. To implement this solution effectively, consider the following best practices:

1. Use Auto Scaling groups to manage the mix of Reserved and Spot Instances.
2. Implement proper error handling and retry mechanisms to manage potential Spot Instance interruptions.
3. Use the capacity-optimized Spot allocation strategy to reduce the likelihood of interruptions.
4. Regularly review and adjust your Reserved Instance commitments based on actual usage patterns.

5. Monitor your application's performance and costs to optimize the balance between Reserved and Spot Instances over time. By following this approach, the company can achieve a good balance between cost-effectiveness and reliability for their production application with variable workloads.

Sources [1] [Amazon EC2 FAQs – AWS] (<https://aws.amazon.com/ec2/faqs/>) [3] [EC2 Fleet and Spot Fleet – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Fleets.html>) [6] [Amazon EC2 container instances for Amazon ECS – Amazon Elastic Container Service] (<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/create-capacity.html>)

解析: Based on the requirements for the company's production application running on Amazon EC2 instances, processing messages from an Amazon SQS queue with unpredictable and intermittent traffic, the most cost-effective solution that meets these requirements is: C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle

additional capacity. Here's why this solution is the most cost-effective while meeting the requirements:

- 1. Cost-effectiveness:
 - Reserved Instances provide significant discounts compared to On-Demand pricing for a committed baseline capacity.
 - Spot Instances offer up to 90% cost savings compared to On-Demand instances for handling variable workloads.
- 2. Handling unpredictable and intermittent traffic:
 - Reserved Instances cover the baseline capacity, ensuring a minimum level of resources is always available.
 - Spot Instances can be used to scale up during traffic spikes, providing additional capacity when needed.
- 3. Continuous processing without downtime:
 - Reserved Instances provide a stable base for continuous processing.
 - By using a mix of instance types and spreading across multiple Availability Zones, the risk of Spot Instance interruptions can be mitigated.
- 4. Flexibility:
 - This hybrid approach allows for adjusting the balance between cost savings and stability based on the application's specific needs.
 - To implement this solution effectively, consider the following best practices:
 1. Use Auto Scaling groups to manage the mix of Reserved and Spot Instances.
 2. Implement proper error handling and retry mechanisms to manage potential Spot Instance interruptions.
 3. Use the capacity-optimized Spot allocation strategy to reduce the likelihood of interruptions.
 4. Regularly review and adjust your Reserved Instance commitments based on actual usage patterns.
 5. Monitor your application's performance and costs to optimize the balance between Reserved and Spot Instances over time. - By following this approach, the company can achieve a good balance between cost-effectiveness and reliability for their production application with variable workloads.

Sources [1] [Amazon EC2 FAQs - AWS] (<https://aws.amazon.com/ec2/faqs/>) [3] [EC2 Fleet and Spot Fleet - Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Fleets.html>) [6] [Amazon EC2 container instances for Amazon ECS - Amazon Elastic Container Service] (<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/create-capacity.html>)

148. Question #168A 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?

- 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.

答案: D

解析: The correct answer is D. Creating a service control policy (SCP) in the root organizational unit allows the security team to set permissions that apply to all accounts within the organization. SCPs are a powerful way to enforce least privilege access across multiple accounts from a central location.

解析: The correct answer is D. Creating a service control policy (SCP) in the root organizational unit allows the security team to set permissions that apply to all accounts within the organization. SCPs are a powerful way to enforce least privilege access across multiple accounts from a central location.

149. Question #169A 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?

- 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.

答案: C

解析: The correct answer is C. AWS Shield Advanced provides DDoS protection for applications running on AWS, including those served through an Application Load Balancer. It includes additional layers of defense against sophisticated attacks and is designed to protect against the most common and sophisticated DDoS attacks.

解析: The correct answer is C. AWS Shield Advanced provides DDoS protection for applications running on AWS, including those served through an Application Load Balancer. It includes additional layers of defense against sophisticated attacks and is designed to protect against the most common and sophisticated DDoS attacks.

150. Question #170A 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?

- 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.

答案: C

解析: The correct answer is C. By configuring AWS WAF (Web Application Firewall) on the Application Load Balancer, the architect can create geolocation-based access control rules that allow or block traffic based on the visitor's country. This can effectively restrict access to the web application to only users from the specified country.

解析: The correct answer is C. By configuring AWS WAF (Web Application Firewall) on the Application Load Balancer, the architect can create geolocation-based access control rules that allow or block traffic based on the visitor's country. This can effectively restrict access to the web application to only users from the specified country.

151. Question #171A 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?

- 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.

答案：B

解析：The correct answer is B. Using Amazon API Gateway in combination with AWS Lambda allows for a serverless architecture that can automatically scale to meet the increased demand during the holiday season. Lambda functions can handle the tax computations in a scalable and cost-effective manner, as they are event-driven and only consume resources when they are actively processing a request.

解析：The correct answer is B. Using Amazon API Gateway in combination with AWS Lambda allows for a serverless architecture that can automatically scale to meet the increased demand during the holiday season. Lambda functions can handle the tax computations in a scalable and cost-effective manner, as they are event-driven and only consume resources when they are actively processing a request.

152. Question #172A 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?

- 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.

答案: C

解析: The correct answer is C. Configuring a CloudFront field-level encryption profile provides an additional layer of security that ensures sensitive data is encrypted and can only be decrypted by specific applications that have the necessary credentials. This encryption is applied at the field level, protecting the data as it passes through the application stack.

解析: The correct answer is C. Configuring a CloudFront field-level encryption profile provides an additional layer of security that ensures sensitive data is encrypted and can only be decrypted by specific applications that have the necessary credentials. This encryption is applied at the field level, protecting the data as it passes through the application stack.

153. Question #173A 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 are 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?

- 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.

答案：B

解析：The correct answer is B. Amazon CloudFront is a CDN that can cache the content of the S3 bucket and serve it from edge locations around the world, reducing the load on the origin S3 bucket and improving the user experience by providing low-latency access to the media files.

解析：The correct answer is B. Amazon CloudFront is a CDN that can cache the content of the S3 bucket and serve it from edge locations around the world, reducing the load on the origin S3 bucket and improving the user experience by providing low-latency access to the media files.

154. Question #174A 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?

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.

答案：B

解析：The correct answer is B. By modifying the Auto Scaling group to span two Availability Zones, the architect ensures that the front-end web servers are deployed across multiple zones, which provides high availability in the event of a failure in one zone. This approach does not require changes to the application and leverages the built-in

redundancy of multi-AZ deployments.

解析: The correct answer is B. By modifying the Auto Scaling group to span two Availability Zones, the architect ensures that the front-end web servers are deployed across multiple zones, which provides high availability in the event of a failure in one zone. This approach does not require changes to the application and leverages the built-in redundancy of multi-AZ deployments.

155. Question #175An 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?

- 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.

答案: B

解析: The correct answer is B. Amazon RDS Proxy can help manage the database connections more efficiently by creating a connection pool, which reduces the number of open connections and the load on the database. This can prevent timeout errors without requiring significant

changes to the application.

解析: The correct answer is B. Amazon RDS Proxy can help manage the database connections more efficiently by creating a connection pool, which reduces the number of open connections and the load on the database. This can prevent timeout errors without requiring significant changes to the application.

156. Question #176An 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?

- 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.

答案: A

解析: The correct answer is A. A VPC endpoint for DynamoDB allows the EC2 instances to communicate with DynamoDB using private IP addresses, ensuring that the traffic stays within the AWS network. This is the most secure method as it does not involve routing traffic through a public internet gateway or a NAT device.

解析: The correct answer is A. A VPC endpoint for DynamoDB allows the EC2 instances to communicate with DynamoDB using private IP addresses, ensuring that the traffic stays within the AWS network. This is the most secure method as it does not involve routing traffic through a public internet gateway or a NAT device.

157. Question #177An 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?

- 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.

答案：B

解析：The correct answer is B. Amazon DynamoDB Accelerator (DAX) is an in-memory cache that can significantly improve the read performance of a DynamoDB table without requiring changes to the application. DAX is designed to reduce latency for read-intensive workloads and can be used as a caching layer for DynamoDB.

解析：The correct answer is B. Amazon DynamoDB Accelerator (DAX) is an in-memory cache that can significantly improve the read performance of a DynamoDB table without requiring changes to the application. DAX is designed to reduce latency for read-intensive workloads and can be used as a caching layer for DynamoDB.

158. Question #178A 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?
- 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.

答案：A

解析：The correct answer is A. AWS Backup is a fully managed service that can be used to automate and centralize the process of creating backups across AWS Regions, including both EC2 instances and RDS databases. This

approach requires the least operational overhead as it does not involve manual snapshot management or the configuration of replication across Regions.

解析: The correct answer is A. AWS Backup is a fully managed service that can be used to automate and centralize the process of creating backups across AWS Regions, including both EC2 instances and RDS databases. This approach requires the least operational overhead as it does not involve manual snapshot management or the configuration of replication across Regions.

159. Question #179A 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?

- 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.

答案: A

解析: The correct answer is A. By creating an IAM role with the necessary permissions to access the Parameter Store and decrypt the parameter using a KMS key, the architect can securely manage access to the database credentials. Assigning this role to the EC2 instance ensures that the

application running on the instance can retrieve the required credentials without exposing them.

解析：The correct answer is A. By creating an IAM role with the necessary permissions to access the Parameter Store and decrypt the parameter using a KMS key, the architect can securely manage access to the database credentials. Assigning this role to the EC2 instance ensures that the application running on the instance can retrieve the required credentials without exposing them.

160. Question #181A 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?

- 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.

答案：A

解析: The correct answer is A. Amazon SQS is a fully managed message queuing service that enables microservices to communicate asynchronously. Data producers can send messages to the SQS queue, and data consumers can process these messages independently, making it a suitable choice for decoupled communication between microservices.

解析: The correct answer is A. Amazon SQS is a fully managed message queuing service that enables microservices to communicate asynchronously. Data producers can send messages to the SQS queue, and data consumers can process these messages independently, making it a suitable choice for decoupled communication between microservices.

161. Question #182A 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?

- 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.

答案: B

解析: The correct answer is B. Amazon RDS with Multi-AZ functionality provides a high availability configuration that maintains a synchronous standby replica in a different Availability Zone. This setup ensures that data is synchronously replicated across instances, which helps to minimize data loss and provides a highly available database solution.

解析: The correct answer is B. Amazon RDS with Multi-AZ functionality provides a high availability configuration that maintains a synchronous

standby replica in a different Availability Zone. This setup ensures that data is synchronously replicated across instances, which helps to minimize data loss and provides a highly available database solution.

162. Question #183A 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?
- 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.

答案: A

解析: The correct answer is A. This solution leverages a serverless architecture by using Amazon S3 for hosting static content, Amazon API Gateway and AWS Lambda for dynamic content generation, and Amazon DynamoDB with on-demand capacity for the database. This approach minimizes server maintenance and patching, provides high availability, and can quickly scale read and write capacity to meet fluctuating user demand.

解析: The correct answer is A. This solution leverages a serverless architecture by using Amazon S3 for hosting static content, Amazon API Gateway and AWS Lambda for dynamic content generation, and Amazon DynamoDB with on-demand capacity for the database. This approach minimizes server maintenance and patching, provides high availability, and can quickly scale read and write capacity to meet fluctuating user demand.

163. Question #184A 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?

- 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.

答案: A

解析: The correct answer is A. By configuring the Lambda function to run within the VPC and associating it with the appropriate security group, the function can access resources in the VPC, including the private subnet where the database resides. This setup allows the Lambda function to use the Direct Connect connection to communicate with the on-premises data center without the need for a VPN or an Elastic IP address.

解析: The correct answer is A. By configuring the Lambda function to run within the VPC and associating it with the appropriate security group,

the function can access resources in the VPC, including the private subnet where the database resides. This setup allows the Lambda function to use the Direct Connect connection to communicate with the on-premises data center without the need for a VPN or an Elastic IP address.

164. Question #185A 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?

- 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.

答案：B

解析：The correct answer is B. To grant the necessary permissions to an ECS application to access Amazon S3, the architect should create an IAM role with the required S3 permissions and then specify that IAM role as the taskRoleArn in the task definition of the ECS application. This allows the ECS tasks to assume the role and use the permissions associated with it to interact with S3.

解析：The correct answer is B. To grant the necessary permissions to an ECS application to access Amazon S3, the architect should create an IAM role with the required S3 permissions and then specify that IAM role as the taskRoleArn in the task definition of the ECS application. This allows the ECS tasks to assume the role and use the permissions associated with it to interact with S3.

165. Question #186A 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?

- 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.

答案: B

解析: Option B is the correct answer. Amazon FSx for Windows File Server is a fully managed file storage service that provides a native Windows file system that can be accessed over the SMB protocol. It is specifically designed for use with Windows-based applications, and it can be easily integrated with existing applications by mounting the file system to each EC2 instance.

解析: Option B is the correct answer. Amazon FSx for Windows File Server is a fully managed file storage service that provides a native Windows file system that can be accessed over the SMB protocol. It is specifically designed for use with Windows-based applications, and it can be easily integrated with existing applications by mounting the file system to each EC2 instance.

166. Question #188A 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?

- 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.

答案：A

解析：Option A is the correct answer. AWS Transfer Family is a fully managed service that can be used to set up and run SFTP servers, which can be easily integrated with Amazon S3, providing a highly available and scalable solution for SFTP file transfers.

解析：Option A is the correct answer. AWS Transfer Family is a fully managed service that can be used to set up and run SFTP servers, which can be easily integrated with Amazon S3, providing a highly available and scalable solution for SFTP file transfers.

167. Question #190A 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?

- 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.

答案：B

解析：Option B is the correct answer. AWS Elastic Beanstalk is a fully managed service that can automatically handle the deployment, scaling, and monitoring of web applications. The use of URL swapping allows for easy testing of new features by switching between environments.

解析：Option B is the correct answer. AWS Elastic Beanstalk is a fully managed service that can automatically handle the deployment, scaling, and monitoring of web applications. The use of URL swapping allows for easy testing of new features by switching between environments.

168. Question #191A 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?

- 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.

答案：A

解析：Option A is the correct answer. By creating a read replica, the reporting queries can be offloaded from the primary database instance to the replica, which helps to eliminate timeouts during order processing

without hindering the employees' ability to perform their queries.

解析: Option A is the correct answer. By creating a read replica, the reporting queries can be offloaded from the primary database instance to the replica, which helps to eliminate timeouts during order processing without hindering the employees' ability to perform their queries.

169. Question #193A 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?

- 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.

答案: B

解析: Option B is the correct answer. Amazon ElastiCache for Redis can be used to cache frequently read data, thereby reducing the number of reads from the Amazon RDS databases. Redis is a high-performance in-memory cache that can help in reducing database load and improving application performance.

解析: Option B is the correct answer. Amazon ElastiCache for Redis can be used to cache frequently read data, thereby reducing the number of reads from the Amazon RDS databases. Redis is a high-performance in-memory cache that can help in reducing database load and improving application performance.

170. Question #194A 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?

- 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.

答案：A

解析：old(C)→new(A) old: Option C is the correct answer. By launching EC2 instances in different AWS Regions and setting up database replication, the company can achieve high availability and automatic failover in the event of a disruptive event in one region. This cross-region setup ensures that the application can continue to operate even if one entire region goes down. new: waiting...

解析：old(C)→new(A) old: Option C is the correct answer. By launching EC2 instances in different AWS Regions and setting up database replication, the company can achieve high availability and automatic failover in the event of a disruptive event in one region. This cross-region setup ensures that the application can continue to operate even if one entire region goes down. new: waiting...

171. Question #195 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?
- 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.

答案: C

解析: Option C is the correct answer. By using Amazon SQS, the system can decouple the order processing and ensure that messages are not lost during a system outage. SQS is a robust, distributed queue system that can handle large numbers of requests and ensure that each message is processed exactly once.

解析: Option C is the correct answer. By using Amazon SQS, the system can decouple the order processing and ensure that messages are not lost during a system outage. SQS is a robust, distributed queue system that can handle large numbers of requests and ensure that each message is processed exactly once.

172. Question #196A 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?

- 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.

答案：D

解析：Option D is the correct answer. By using DynamoDB's TTL (Time to Live) feature, the company can automatically delete items from the table that are older than 30 days, without the need for additional EC2 instances, Lambda functions, or manual intervention.

解析：Option D is the correct answer. By using DynamoDB's TTL (Time to Live) feature, the company can automatically delete items from the table that are older than 30 days, without the need for additional EC2 instances, Lambda functions, or manual intervention.

173. Question #198A 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?

- 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.

答案：D

解析：Option D is the correct answer. Amazon EKS can be used to run Kubernetes clusters on AWS, and AWS Fargate can be used to run containerized applications without managing the underlying infrastructure. Amazon DocumentDB is a fully managed database service that is compatible with MongoDB, which allows the company to migrate their database without changing the application code or deployment methods.

解析：Option D is the correct answer. Amazon EKS can be used to run Kubernetes clusters on AWS, and AWS Fargate can be used to run containerized applications without managing the underlying infrastructure. Amazon DocumentDB is a fully managed database service that is compatible with MongoDB, which allows the company to migrate their database without changing the application code or deployment methods.

174. Question #199A 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?

- 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.

答案：B

解析：Option B is the correct answer. Amazon Transcribe can be used for multiple speaker recognition and can generate transcript files. These files can be stored in Amazon S3 for long-term storage. Amazon Athena can then be used to query and analyze the stored transcript files using SQL.

解析：Option B is the correct answer. Amazon Transcribe can be used for multiple speaker recognition and can generate transcript files. These files can be stored in Amazon S3 for long-term storage. Amazon Athena can then be used to query and analyze the stored transcript files using SQL.

175. Question #200A 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?

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.

答案：D

解析：Option D is the correct answer. By configuring an Amazon Cognito user pool authorizer in API Gateway, the company can leverage Amazon Cognito's existing user management capabilities to control access to the REST API with minimal operational overhead and without the need to

develop custom authorization logic.

解析: Option D is the correct answer. By configuring an Amazon Cognito user pool authorizer in API Gateway, the company can leverage Amazon Cognito's existing user management capabilities to control access to the REST API with minimal operational overhead and without the need to develop custom authorization logic.

176. Question #201A 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?

- 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.

答案: B

解析: Option B is the correct answer. Amazon Pinpoint can be used to send SMS messages and can be configured to send events to an Amazon Kinesis data stream. This allows for the analysis and archiving of the SMS responses for a year, as required.

解析: Option B is the correct answer. Amazon Pinpoint can be used to send SMS messages and can be configured to send events to an Amazon Kinesis data stream. This allows for the analysis and archiving of the SMS responses for a year, as required.

177. Question #202A 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?

- 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.

答案: B

解析: Option B is the correct answer. By using a customer managed key in AWS KMS and enabling automatic key rotation, the company can ensure that the data is encrypted with a key that is automatically rotated every year, meeting the requirement with minimal operational overhead.

解析: Option B is the correct answer. By using a customer managed key in AWS KMS and enabling automatic key rotation, the company can ensure that the data is encrypted with a key that is automatically rotated every year, meeting the requirement with minimal operational overhead.

178. Question #203 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?

- 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.

答案：D

解析：Option D is the correct answer. By adding an Auto Scaling group for the application that sends meeting invitations and configuring it to scale based on the depth of the SQS queue, the system can automatically adjust the number of instances processing the messages, thereby reducing the delivery time for meeting invitations as the queue depth increases.

解析：Option D is the correct answer. By adding an Auto Scaling group for the application that sends meeting invitations and configuring it to scale based on the depth of the SQS queue, the system can automatically adjust the number of instances processing the messages, thereby reducing the delivery time for meeting invitations as the queue depth increases.

179. Question #204 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?

- 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.

答案：C

解析：Option C is the correct answer. AWS Lake Formation provides a centralized repository for managing data analytics resources and allows for fine-grained access control to data stored in Amazon S3 and RDS. By creating a data lake and using Lake Formation's access controls, the company can meet the requirements for data availability, permission management, and operational efficiency.

解析：Option C is the correct answer. AWS Lake Formation provides a centralized repository for managing data analytics resources and allows for fine-grained access control to data stored in Amazon S3 and RDS. By creating a data lake and using Lake Formation's access controls, the company can meet the requirements for data availability, permission management, and operational efficiency.

180. Question #205A 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?

- 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.

答案: C

解析: Option C is the correct answer. By creating a private Amazon S3 bucket and configuring it to be accessed by CloudFront using an OAI, the company can serve static content through CloudFront efficiently. Using the AWS CLI for uploads ensures secure transfers, and the use of S3 as the origin provides a resilient and scalable solution for hosting the website content.

解析: Option C is the correct answer. By creating a private Amazon S3 bucket and configuring it to be accessed by CloudFront using an OAI, the company can serve static content through CloudFront efficiently. Using the AWS CLI for uploads ensures secure transfers, and the use of S3 as the origin provides a resilient and scalable solution for hosting the website content.

181. Question #206A 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?
- 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.

答案: C

解析: Option C is the correct answer. By using Amazon EventBridge to create a rule that triggers on the CreateImage API call, the company can set up a direct and efficient alerting mechanism through Amazon SNS with minimal operational overhead. This solution avoids the need for additional querying or processing of logs, making it the most straightforward and least resource-intensive option.

解析: Option C is the correct answer. By using Amazon EventBridge to create a rule that triggers on the CreateImage API call, the company can set up a direct and efficient alerting mechanism through Amazon SNS with minimal operational overhead. This solution avoids the need for additional querying or processing of logs, making it the most straightforward and least resource-intensive option.

182. Question #207A 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?

- 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.

答案: D

解析: Option D is the correct answer. By using Amazon SQS in combination with AWS Lambda, the system can decouple the request ingestion from the database writes. This allows the Lambda function to queue incoming requests and process them asynchronously, which can help to manage the load on DynamoDB and prevent data loss during periods of high traffic or throttling.

解析: Option D is the correct answer. By using Amazon SQS in combination with AWS Lambda, the system can decouple the request ingestion from the database writes. This allows the Lambda function to queue incoming requests and process them asynchronously, which can help to manage the load on DynamoDB and prevent data loss during periods of high traffic or throttling.

183. Question #209A 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?

- 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.

答案：A

解析：Option A is the correct answer. Amazon ElastiCache, specifically using Redis or Memcached, can be used as a distributed cache to store session data. This allows session information to be shared across multiple EC2 instances in different Availability Zones, which is necessary for an application that requires distributed session management.

解析：Option A is the correct answer. Amazon ElastiCache, specifically using Redis or Memcached, can be used as a distributed cache to store session data. This allows session information to be shared across multiple EC2 instances in different Availability Zones, which is necessary for an application that requires distributed session management.

184. Question #210A 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 ordersThe 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?

- 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.

答案: D

解析: Option D is the correct answer. By using Amazon SQS queues, the system can decouple the order collection from the order fulfillment processes, which allows for better scaling and management of the workflows. Configuring the Auto Scaling groups to scale based on a backlog per instance metric ensures that the scaling is done efficiently and in response to the actual workload, optimizing the use of AWS resources.

解析: Option D is the correct answer. By using Amazon SQS queues, the system can decouple the order collection from the order fulfillment processes, which allows for better scaling and management of the workflows. Configuring the Auto Scaling groups to scale based on a backlog per instance metric ensures that the scaling is done efficiently and in response to the actual workload, optimizing the use of AWS resources.

185. Question #211A 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?

- 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.

答案: D

解析: Option D is the correct answer. AWS Resource Groups Tag Editor allows for searching and reporting on resources across all AWS services and Regions based on their tags. This provides a centralized and efficient way to identify all resources tagged with a specific application name, meeting the requirement for a quick solution.

解析: Option D is the correct answer. AWS Resource Groups Tag Editor allows for searching and reporting on resources across all AWS services and Regions based on their tags. This provides a centralized and efficient way to identify all resources tagged with a specific application name, meeting the requirement for a quick solution.

186. Question #212A 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?

- A. S3 Intelligent-Tiering
- B. S3 Glacier Instant Retrieval
- C. S3 Standard

D. S3 Standard-Infrequent Access (S3 Standard-IA)

答案：A

解析：Based on the requirements provided, the most suitable S3 storage class for the company's needs is: A. S3 Intelligent-Tiering Here's why S3 Intelligent-Tiering is the best choice for this scenario:

- 1. Variable access pattern: The company mentioned that the S3 access pattern for the data is variable and changes rapidly. S3 Intelligent-Tiering is designed specifically for data with unknown, changing, or unpredictable access patterns.
- 2. Immediate availability: The data must be immediately available, which S3 Intelligent-Tiering provides. It offers millisecond access to data, similar to S3 Standard.
- 3. 3-month retention: The data needs to remain accessible for up to 3 months. S3 Intelligent-Tiering has no minimum storage duration requirement, making it suitable for this timeframe.
- 4. Cost-effectiveness: S3 Intelligent-Tiering automatically moves objects between two access tiers (frequent and infrequent access) based on changing access patterns. This optimization helps reduce storage costs without impacting performance or operational overhead.
- 5. No impact on retrieval time: S3 Intelligent-Tiering maintains low-latency and high-throughput performance of S3 Standard, ensuring that the retrieval time is not increased.
- 6. Suitable for varying object sizes: The exported database objects range from 2 GB to 5 GB, which falls within the optimal range for S3 Intelligent-Tiering. By choosing S3 Intelligent-Tiering, the company can benefit from automatic cost optimization without sacrificing performance or immediate access to their data.

This storage class will adapt to the changing access patterns of the exported database files, ensuring the most cost-effective storage solution while meeting all the stated requirements.

Sources [1] [Analyze access patterns and use the most cost-effective Amazon S3 storage class | AWS Storage Blog] (<https://aws.amazon.com/blogs/storage/analyze-access-patterns-and-use-the-most-cost-effective-amazon-s3-storage-class/>) [3] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>) [6] [Understanding and managing Amazon S3 storage classes – Amazon Simple Storage Service] (<http://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>)

解析: Based on the requirements provided, the most suitable S3 storage class for the company's needs is: A. S3 Intelligent-Tiering Here's why S3 Intelligent-Tiering is the best choice for this scenario:

- 1. Variable access pattern: The company mentioned that the S3 access pattern for the data is variable and changes rapidly. S3 Intelligent-Tiering is designed specifically for data with unknown, changing, or unpredictable access patterns.
- 2. Immediate availability: The data must be immediately available, which S3 Intelligent-Tiering provides. It offers millisecond access to data, similar to S3 Standard.
- 3. 3-month retention: The data needs to remain accessible for up to 3 months. S3 Intelligent-Tiering has no minimum storage duration requirement, making it suitable for this timeframe.
- 4. Cost-effectiveness: S3 Intelligent-Tiering automatically moves objects between two access tiers (frequent and infrequent access) based on changing access patterns. This optimization helps reduce storage costs without impacting performance or operational overhead.
- 5. No impact on retrieval time: S3 Intelligent-Tiering maintains low-latency and high-throughput performance of S3 Standard, ensuring that the retrieval time is not increased.
- 6. Suitable for varying object sizes: The exported database objects range from 2 GB to 5 GB, which falls within the optimal range for S3 Intelligent-Tiering. By choosing S3 Intelligent-Tiering, the company can benefit from automatic cost optimization without sacrificing performance or immediate access to their data. This storage class will adapt to the changing access patterns of the exported database files, ensuring the most cost-effective storage solution while meeting all the stated requirements.

Sources [1] [Analyze access patterns and use the most cost-effective Amazon S3 storage class | AWS Storage Blog] (<https://aws.amazon.com/blogs/storage/analyze-access-patterns-and-use-the-most-cost-effective-amazon-s3-storage-class/>) [3] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>) [6] [Understanding and managing Amazon S3 storage classes – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>)

187. Question #213A 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?

- 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.

答案：A

解析：Option A is the correct answer. AWS WAF (Web Application Firewall) can be configured to filter malicious traffic and protect the ALB against common application-level attacks. This solution aligns with the company's need to reduce the operational burden of managing security, as AWS WAF is a managed service that requires minimal configuration and maintenance.

解析：Option A is the correct answer. AWS WAF (Web Application Firewall) can be configured to filter malicious traffic and protect the ALB against common application-level attacks. This solution aligns with the company's need to reduce the operational burden of managing security, as AWS WAF is a managed service that requires minimal configuration and maintenance.

188. Question #214A 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?

- 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.

答案：B

解析：Option B is the correct answer. AWS Glue is a fully managed ETL service that can be used to create crawlers and ETL jobs with minimal development effort. Glue can automatically discover data stored across various data sources, and it can convert .csv files to Parquet format without the need for extensive coding or the management of clusters or batch jobs.

解析：Option B is the correct answer. AWS Glue is a fully managed ETL service that can be used to create crawlers and ETL jobs with minimal development effort. Glue can automatically discover data stored across various data sources, and it can convert .csv files to Parquet format without the need for extensive coding or the management of clusters or batch jobs.

189. Question #215A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data needs to be accessible for infrequent regulatory requests and must be retained for 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?

- 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.

答案：A

解析：Option A is the correct answer. AWS Snowball is a service that allows for the physical transfer of large amounts of data into and out of AWS by using secure appliances. For a one-time migration of 700 TB of data, Snowball would be more cost-effective than maintaining a VPN or Direct Connect connection for the entire month, especially considering the relatively low bandwidth available. After the initial transfer, a lifecycle policy can transition the files to Amazon S3 Glacier Deep Archive for long-term, cost-effective storage.

解析：Option A is the correct answer. AWS Snowball is a service that allows for the physical transfer of large amounts of data into and out of AWS by using secure appliances. For a one-time migration of 700 TB of data, Snowball would be more cost-effective than maintaining a VPN or Direct Connect connection for the entire month, especially considering the relatively low bandwidth available. After the initial transfer, a lifecycle policy can transition the files to Amazon S3 Glacier Deep Archive for long-term, cost-effective storage.

190. Question #216A 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?

- 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.

答案：B

解析：Option B is the correct answer. By enabling default encryption on the S3 bucket and using S3 Inventory to identify unencrypted objects, followed by an S3 Batch Operations job to encrypt these objects, the architect can efficiently secure existing data without the need for manual intervention or the resource-intensive process of downloading and re-uploading all objects.

解析：Option B is the correct answer. By enabling default encryption on the S3 bucket and using S3 Inventory to identify unencrypted objects, followed by an S3 Batch Operations job to encrypt these objects, the architect can efficiently secure existing data without the need for manual intervention or the resource-intensive process of downloading and re-uploading all objects.

191. Question #217A 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?

- 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.

答案：A

解析：Option A is the correct answer. By deploying the application in an active-passive configuration with Amazon Route 53 managing the failover, the company can achieve the required disaster recovery setup. An Aurora Replica in a second AWS Region provides a warm standby that can be promoted to handle read and write operations in the event of a failure, aligning with the acceptable downtime and data loss parameters.

解析：Option A is the correct answer. By deploying the application in an active-passive configuration with Amazon Route 53 managing the failover, the company can achieve the required disaster recovery setup. An Aurora Replica in a second AWS Region provides a warm standby that can be promoted to handle read and write operations in the event of a failure, aligning with the acceptable downtime and data loss parameters.

192. Question #219A 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?

- 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.

答案: D

解析: Option D is the correct answer. Since the application is stateful and requires in-memory processing, switching to R5 instances, which are optimized for memory-intensive tasks, can improve performance.

Additionally, deploying the Amazon CloudWatch agent to generate custom latency metrics allows for more granular monitoring and capacity planning, leading to a more operationally efficient solution.

解析: Option D is the correct answer. Since the application is stateful and requires in-memory processing, switching to R5 instances, which are optimized for memory-intensive tasks, can improve performance.

Additionally, deploying the Amazon CloudWatch agent to generate custom latency metrics allows for more granular monitoring and capacity planning, leading to a more operationally efficient solution.

193. Question #220A 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 invoke to deliver the

requirements at the lowest cost?

- 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

答案: B

解析: Option B is the correct solution as it involves using AWS Lambda, which is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources for you. This means you don't need to provision or manage servers, which makes it a cost-effective choice for handling variable and infrequent requests. AWS Glue (Option A) is more suited for data integration tasks and not for handling direct user requests. Options C and D, involving containerized services on Amazon EKS or Amazon ECS, would require more overhead and management, leading to higher costs for the scenario described.

解析: Option B is the correct solution as it involves using AWS Lambda, which is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources for you. This means you don't need to provision or manage servers, which makes it a cost-effective choice for handling variable and infrequent requests. AWS Glue (Option A) is more suited for data integration tasks and not for handling direct user requests. Options C and D, involving containerized services on Amazon EKS or Amazon ECS, would require more overhead and management, leading to higher costs for the scenario described.

194. Question #221A 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?

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

答案: D

解析: Option D, Amazon S3, is the most cost-effective solution for storing log files that need to be retained for a long period of time. S3 is designed to provide durable and highly available storage, with features that support long-term data retention at a lower cost compared to traditional EBS volumes (Option A) or EFS file systems (Option B). S3 also allows for concurrent access to the files, which is necessary for the reporting tool. Instance store (Option C) is not suitable for this use case as it is ephemeral storage tied to the lifecycle of the EC2 instance.

解析: Option D, Amazon S3, is the most cost-effective solution for storing log files that need to be retained for a long period of time. S3 is designed to provide durable and highly available storage, with features that support long-term data retention at a lower cost compared to traditional EBS volumes (Option A) or EFS file systems (Option B). S3 also allows for concurrent access to the files, which is necessary for the reporting tool. Instance store (Option C) is not suitable for this use case as it is ephemeral storage tied to the lifecycle of the EC2 instance.

195. Question #222A 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?

- A. Create an IAM role in the company's account to delegate access to the vendor's IAM role.
- 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.

答案：A

解析：Option A is the correct approach as it allows the company to create an IAM role in their account that can be assumed by the vendor's IAM users or roles. This is a secure method of granting access without sharing account credentials and adheres to the principle of least privilege. The vendor's IAM role can be given the necessary permissions to perform the required tasks within the company's AWS account. Options B and C are less secure as they involve sharing credentials or adding users directly. Option D is incorrect because it does not relate to granting access from an external vendor's AWS account to the company's AWS account.

解析：Option A is the correct approach as it allows the company to create an IAM role in their account that can be assumed by the vendor's IAM users or roles. This is a secure method of granting access without sharing account credentials and adheres to the principle of least privilege. The vendor's IAM role can be given the necessary permissions to perform the required tasks within the company's AWS account. Options B and C are less secure as they involve sharing credentials or adding users directly. Option D is incorrect because it does not relate to granting access from an external vendor's AWS account to the company's AWS account.

196. Question #225A 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?

- 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.

答案：B

解析：Option B is the correct solution for building a highly available data ingestion solution with minimal operational overhead. Amazon Kinesis Data Firehose (Option B) can automatically load streaming data into an Amazon Redshift cluster, which is a fully managed, petabyte-scale data warehouse service that enables on-demand analytics using SQL. This integration allows for seamless data ingestion and analytics at scale with low operational overhead.

解析：Option B is the correct solution for building a highly available data ingestion solution with minimal operational overhead. Amazon Kinesis Data Firehose (Option B) can automatically load streaming data into an Amazon Redshift cluster, which is a fully managed, petabyte-scale data warehouse service that enables on-demand analytics using SQL. This integration allows for seamless data ingestion and analytics at scale with low operational overhead.

197. Question #227A 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?

- 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.

答案：B

解析：The most cost-effective solution to delete objects older than 3 years, considering the provided options, is to configure the S3 Lifecycle policy to delete previous versions as well as current versions (Option B). This is because S3 Versioning is already enabled, and the S3 Lifecycle policy can be tailored to manage the retention and deletion of objects based on their age, without the need for additional services or manual intervention. Option A is not viable because AWS CloudTrail does not have a native feature to expire objects after a certain period; it only logs API calls. Option C, while possible, would incur additional costs for running a Lambda function and is not as efficient as leveraging the existing S3 Lifecycle policy. Option D does not address the issue of deleting old objects and is related to the ownership of the objects, not their retention policy.

解析：The most cost-effective solution to delete objects older than 3 years, considering the provided options, is to configure the S3 Lifecycle policy to delete previous versions as well as current versions (Option B). This is because S3 Versioning is already enabled, and the S3 Lifecycle policy can be tailored to manage the retention and deletion of objects based on their age, without the need for additional services or manual intervention. Option A is not viable because AWS CloudTrail does not have a native feature to expire objects after a certain period; it only logs API calls. Option C, while possible, would incur additional

costs for running a Lambda function and is not as efficient as leveraging the existing S3 Lifecycle policy. Option D does not address the issue of deleting old objects and is related to the ownership of the objects, not their retention policy.

198. Question #228A 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?

- 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.

答案: C

解析: The solution that best meets the requirements of minimizing the number of connections to the database and ensuring that data is not lost during heavy traffic periods is to use Amazon SQS (Option C). By writing incoming data to an SQS queue, the system can act as a buffer that absorbs traffic spikes and smooths out the flow of data to the database. This approach reduces the direct load on the database and allows for more controlled data processing. Option A might provide a temporary solution by increasing the DB instance size, but it does not address the

underlying issue of connection management and does not ensure data integrity during traffic spikes. Option B, while it provides high availability with Multi-AZ deployment, does not solve the problem of connection management and could lead to increased complexity and data inconsistency. Option D, using SNS, could distribute messages but does not provide the same reliable queuing and load management capabilities as SQS, which is specifically designed for buffering and managing bursts of messages before processing.

解析: The solution that best meets the requirements of minimizing the number of connections to the database and ensuring that data is not lost during heavy traffic periods is to use Amazon SQS (Option C). By writing incoming data to an SQS queue, the system can act as a buffer that absorbs traffic spikes and smooths out the flow of data to the database. This approach reduces the direct load on the database and allows for more controlled data processing. Option A might provide a temporary solution by increasing the DB instance size, but it does not address the underlying issue of connection management and does not ensure data integrity during traffic spikes. Option B, while it provides high availability with Multi-AZ deployment, does not solve the problem of connection management and could lead to increased complexity and data inconsistency. Option D, using SNS, could distribute messages but does not provide the same reliable queuing and load management capabilities as SQS, which is specifically designed for buffering and managing bursts of messages before processing.

199. Question #229A 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?

- 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.

答案: A

解析: Option A, migrating the databases to Amazon Aurora Serverless for Aurora MySQL, is the solution that best meets the requirements. Amazon Aurora Serverless is a fully managed, auto-scaling database service that automatically adjusts to the application's needs and requires no manual intervention for capacity management. It offers improved performance, scaling, and durability with minimal operational effort, which aligns with the company's needs. Option B, while similar to Option A, specifies Aurora PostgreSQL instead of Aurora MySQL, which may not be suitable if the company is using MySQL databases. Option C, combining databases into one larger database, could lead to complexity and does not inherently solve the scaling and management issues. Option D, creating an EC2 Auto Scaling group, does not address the database tier's specific scaling needs and would still require manual management of the databases.

解析: Option A, migrating the databases to Amazon Aurora Serverless for Aurora MySQL, is the solution that best meets the requirements. Amazon Aurora Serverless is a fully managed, auto-scaling database service that automatically adjusts to the application's needs and requires no manual intervention for capacity management. It offers improved performance, scaling, and durability with minimal operational effort, which aligns with the company's needs. Option B, while similar to Option A, specifies Aurora PostgreSQL instead of Aurora MySQL, which may not be suitable if the company is using MySQL databases. Option C, combining databases into one larger database, could lead to complexity and does not inherently solve the scaling and management issues. Option D, creating an EC2 Auto Scaling group, does not address the database tier's specific scaling needs and would still require manual management of the databases.

200. Question #230A 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?

- 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.

答案：C

解析：The solutions architect should recommend Option C, which is to remove the two NAT instances and replace them with two NAT gateways in different Availability Zones. NAT gateways are managed by AWS, providing a higher level of availability and scalability compared to NAT instances. By placing NAT gateways in different Availability Zones, the solution achieves fault tolerance and redundancy, ensuring that the application's network traffic can be maintained even if one Availability Zone experiences an outage. Option A is not as robust because it keeps the NAT gateways in the same Availability Zone, which does not provide fault tolerance across zones. Option B introduces complexity with Auto Scaling and Network Load Balancers for NAT instances, which do not inherently provide the scalability and manageability of NAT gateways. Option D is not recommended because it involves using Spot Instances, which can be terminated by AWS if the spot market price becomes too high or if AWS requires the capacity for other purposes, thus impacting the stability of the network traffic.

解析：The solutions architect should recommend Option C, which is to remove the two NAT instances and replace them with two NAT gateways in different Availability Zones. NAT gateways are managed by AWS, providing a higher level of availability and scalability compared to NAT instances.

By placing NAT gateways in different Availability Zones, the solution achieves fault tolerance and redundancy, ensuring that the application's network traffic can be maintained even if one Availability Zone experiences an outage. Option A is not as robust because it keeps the NAT gateways in the same Availability Zone, which does not provide fault tolerance across zones. Option B introduces complexity with Auto Scaling and Network Load Balancers for NAT instances, which do not inherently provide the scalability and manageability of NAT gateways. Option D is not recommended because it involves using Spot Instances, which can be terminated by AWS if the spot market price becomes too high or if AWS requires the capacity for other purposes, thus impacting the stability of the network traffic.

201. Question #231An 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**?

- 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.

答案: B

解析: old(A)-->new(B) old: The most secure and reliable solution for enabling secure access between EC2 instances in separate VPCs, which are in different AWS accounts, is to set up a VPC peering connection (Option A). **VPC peering allows for direct network communication between the two VPCs over the AWS network, without exposing the traffic to the public internet.** This setup does not have a single point of failure and does not introduce bandwidth concerns, as it uses the existing AWS infrastructure. Option B, VPC gateway endpoints, are used to enable private connections between services in a VPC and AWS services, but they do not facilitate

communication between VPCs. Option C, attaching a virtual private gateway, is part of setting up a VPN connection, which is not necessary when VPC peering can be used. Option D, creating a private virtual interface, is typically used for AWS Direct Connect and not for VPC-to-VPC communication. new: waiting..

解析: old(A)-->new(B) old: The most secure and reliable solution for enabling secure access between EC2 instances in separate VPCs, which are in different AWS accounts, is to set up a VPC peering connection (Option A). VPC peering allows for direct network communication between the two VPCs over the AWS network, without exposing the traffic to the public internet. This setup does not have a single point of failure and does not introduce bandwidth concerns, as it uses the existing AWS infrastructure. Option B, VPC gateway endpoints, are used to enable private connections between services in a VPC and AWS services, but they do not facilitate communication between VPCs. Option C, attaching a virtual private gateway, is part of setting up a VPN connection, which is not necessary when VPC peering can be used. Option D, creating a private virtual interface, is typically used for AWS Direct Connect and not for VPC-to-VPC communication. new: waiting..

202. Question #238A 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?

- 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.

答案：C

解析：The most cost-effective solution for setting up notifications when EC2 instance usage exceeds a certain threshold is to use AWS Budgets (Option C). AWS Budgets allow the creation of custom budgets that can track costs and usage, and they can be set up to alert when costs exceed the defined thresholds. By configuring an Amazon SNS topic, the team can receive notifications promptly, which is a scalable and cost-effective way to monitor and manage AWS spending.

解析：The most cost-effective solution for setting up notifications when EC2 instance usage exceeds a certain threshold is to use AWS Budgets (Option C). AWS Budgets allow the creation of custom budgets that can track costs and usage, and they can be set up to alert when costs exceed the defined thresholds. By configuring an Amazon SNS topic, the team can receive notifications promptly, which is a scalable and cost-effective way to monitor and manage AWS spending.

203. Question #239A 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**?

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 Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
- D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

答案：A

解析：The most operationally efficient way to deploy the Lambda function with the requirements stated is to create an Amazon API Gateway REST API (Option A). API Gateway can be configured to trigger a Lambda function and can be set up with IAM authentication to control access to the HTTPS endpoint. This setup is straightforward, does not require additional services like CloudFront for the sole purpose of authentication, and is a common pattern for creating APIs that trigger Lambda functions.

解析：The most operationally efficient way to deploy the Lambda function with the requirements stated is to create an Amazon API Gateway REST API (Option A). API Gateway can be configured to trigger a Lambda function and can be set up with IAM authentication to control access to the HTTPS endpoint. This setup is straightforward, does not require additional services like CloudFront for the sole purpose of authentication, and is a common pattern for creating APIs that trigger Lambda functions.

204. Question #240A 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?
- 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.

答案: D

解析: The solution that provides the lowest data transfer egress cost is to host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection (Option D). This setup minimizes data transfer costs by keeping all data within the AWS network and avoiding internet egress charges. Direct Connect ensures a private, dedicated network connection between the on-premises infrastructure and the AWS Region, which does not incur data transfer egress fees.

解析: The solution that provides the lowest data transfer egress cost is to host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection (Option D). This setup minimizes data transfer costs by keeping all data within the AWS network and avoiding internet egress charges. Direct Connect ensures a private, dedicated network connection between the on-premises infrastructure and the AWS Region, which does not incur data transfer egress fees.

205. Question #241 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?

- 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.

答案: C

解析: To ensure that the student records database is available and online across multiple AWS Regions at all times with the least amount of operational overhead, the company should migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance and create a read replica in another Region (Option C). This approach provides high availability and data redundancy across different AWS Regions without the need for managing the underlying infrastructure, which reduces operational overhead compared to self-managed PostgreSQL clusters on EC2 (Option A) or manually copying DB snapshots across Regions (Option D). The Multi-AZ feature (Option B) provides high availability within a single Region but does not offer the cross-region redundancy needed for this scenario.

解析: To ensure that the student records database is available and online across multiple AWS Regions at all times with the least amount of operational overhead, the company should migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance and create a read replica in another Region (Option C). This approach provides high availability and data redundancy across different AWS Regions without the need for managing the underlying infrastructure, which reduces operational overhead compared to self-managed PostgreSQL clusters on EC2 (Option A) or manually copying DB snapshots across Regions (Option D). The Multi-AZ feature (Option B) provides high availability within a single Region but does not offer the cross-region redundancy needed for this scenario.

206. Question #242A 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?

- A. Simple routing policy
- B. Latency routing policy

- C. Multivalue routing policy
- D. Geolocation routing policy

答案: C

解析: To meet the requirement of returning the IP addresses of all healthy EC2 instances in response to DNS queries, a Multivalue routing policy (Option C) should be used. This policy type allows for the return of multiple IP addresses for a single DNS query, which is suitable when all healthy instances need to be discovered through DNS. In contrast, a Simple routing policy (Option A) would only return a single IP address, Latency routing policy (Option B) is designed to minimize the latency to a single resource, and Geolocation routing policy (Option D) directs users to the closest resource based on geographic location, which may not be necessary or desirable in this scenario.

解析: To meet the requirement of returning the IP addresses of all healthy EC2 instances in response to DNS queries, a Multivalue routing policy (Option C) should be used. This policy type allows for the return of multiple IP addresses for a single DNS query, which is suitable when all healthy instances need to be discovered through DNS. In contrast, a Simple routing policy (Option A) would only return a single IP address, Latency routing policy (Option B) is designed to minimize the latency to a single resource, and Geolocation routing policy (Option D) directs users to the closest resource based on geographic location, which may not be necessary or desirable in this scenario.

207. Question #243A 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?

- 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.

答案: A

解析: To provide minimum latency access to the data files stored in an Amazon S3 bucket for on-premises applications at various clinics, the solutions architect should recommend deploying an AWS Storage Gateway file gateway (Option A). The file gateway acts as a bridge between the on-premises environment and AWS cloud storage, allowing applications to access data directly via a mounted file system while the data is stored and managed in S3. This approach ensures low-latency access and does not require data migration or changes to the existing on-premises infrastructure.

解析: To provide minimum latency access to the data files stored in an Amazon S3 bucket for on-premises applications at various clinics, the solutions architect should recommend deploying an AWS Storage Gateway file gateway (Option A). The file gateway acts as a bridge between the on-premises environment and AWS cloud storage, allowing applications to access data directly via a mounted file system while the data is stored and managed in S3. This approach ensures low-latency access and does not require data migration or changes to the existing on-premises infrastructure.

208. Question #244A 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?

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.

答案：C

解析：To ensure high availability and scalability for the website platform, the solutions architect should recommend moving the database to Amazon Aurora with a read replica in another Availability Zone (Option C). This provides database resilience and performance. Additionally, creating an AMI from the EC2 instance and configuring an Application Load Balancer in two Availability Zones, along with an Auto Scaling group that uses the AMI, allows for automatic scaling based on demand and maintains high availability across different zones. This setup minimizes downtime and provides a robust solution for unpredictable workloads.

解析：To ensure high availability and scalability for the website platform, the solutions architect should recommend moving the database to Amazon Aurora with a read replica in another Availability Zone (Option C). This provides database resilience and performance. Additionally, creating an AMI from the EC2 instance and configuring an Application Load Balancer in two Availability Zones, along with an Auto Scaling group that uses the AMI, allows for automatic scaling based on demand and maintains high availability across different zones. This setup minimizes downtime and provides a robust solution for unpredictable workloads.

209. Question #245A 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?

- 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.

答案：D

解析：To configure the development environment most cost-effectively, the solutions architect should reduce the maximum number of EC2 instances in the development environment's Auto Scaling group (Option D). This allows the development environment to scale down when not under heavy load, thus reducing costs. The development environment typically does not require the same level of resources as the production environment, so limiting the maximum instances helps in controlling expenses. Options A and B do not directly address cost reduction, and Option C may not be as cost-effective since it involves changing instance sizes which may not be necessary for the development environment's workload.

解析：To configure the development environment most cost-effectively, the solutions architect should reduce the maximum number of EC2 instances in the development environment's Auto Scaling group (Option D). This allows the development environment to scale down when not under heavy load, thus reducing costs. The development environment typically does not require the same level of resources as the production environment, so limiting the maximum instances helps in controlling expenses. Options A and B do not directly address cost reduction, and Option C may not be as cost-effective since it involves changing instance sizes which may not be necessary for the development environment's workload.

210. Question #246A 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?

- 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.

答案: D

解析: To resolve the issue of internet traffic not reaching the EC2 instances, the solutions architect should create public subnets in each Availability Zone and associate these with the ALB (Option D). This allows the ALB to have a route to the internet for incoming traffic. Additionally, updating the route tables for the public subnets with a route to the private subnets ensures that the traffic can be directed to the EC2 instances in their private subnets. This configuration maintains the privacy of the EC2 instances while allowing them to receive traffic from the internet through the ALB.

解析: To resolve the issue of internet traffic not reaching the EC2 instances, the solutions architect should create public subnets in each Availability Zone and associate these with the ALB (Option D). This allows the ALB to have a route to the internet for incoming traffic. Additionally, updating the route tables for the public subnets with a route to the private subnets ensures that the traffic can be directed to

the EC2 instances in their private subnets. This configuration maintains the privacy of the EC2 instances while allowing them to receive traffic from the internet through the ALB.

211. Question #248A 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?

- 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.

答案: D

解析: To improve system performance and scale based on user load, the solutions architect should implement a solution that decouples the job request process from the processing instances. This can be achieved by routing incoming requests to an Amazon SQS queue (Option D). By configuring an EC2 Auto Scaling group based on the queue size, the system can automatically scale in or out according to the number of messages in the queue. This ensures that the CPU utilization remains optimal, and all job requests are processed without delays. Additionally, updating the software to read from the queue ensures that the processing is aligned with the available capacity.

解析: To improve system performance and scale based on user load, the solutions architect should implement a solution that decouples the job request process from the processing instances. This can be achieved by

routing incoming requests to an Amazon SQS queue (Option D). By configuring an EC2 Auto Scaling group based on the queue size, the system can automatically scale in or out according to the number of messages in the queue. This ensures that the CPU utilization remains optimal, and all job requests are processed without delays. Additionally, updating the software to read from the queue ensures that the processing is aligned with the available capacity.

212. Question #249A 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?

- 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.

答案: D

解析: old(C) --> new(D) old: The solution that meets the requirements of providing shared storage with SMB access and is fully managed by AWS is Amazon FSx for Windows File Server (Option C). This service is designed to provide a scalable, high-performance file system that is accessible via the SMB protocol, which is ideal for media applications that require shared access to data. In contrast, AWS Storage Gateway (Option A) is a hybrid storage solution that connects on-premises applications with cloud-based storage, but it does not natively support SMB file shares. Setting up an EC2 instance (Option B) requires management of the Windows file share, which does not align with the requirement for a fully managed

solution. Amazon S3 (Option D) is an object storage service that does not provide file system semantics or native SMB access. new: waiting...

解析: old(C)-->new(D) old: The solution that meets the requirements of providing shared storage with SMB access and is fully managed by AWS is Amazon FSx for Windows File Server (Option C). This service is designed to provide a scalable, high-performance file system that is accessible via the SMB protocol, which is ideal for media applications that require shared access to data. In contrast, AWS Storage Gateway (Option A) is a hybrid storage solution that connects on-premises applications with cloud-based storage, but it does not natively support SMB file shares. Setting up an EC2 instance (Option B) requires management of the Windows file share, which does not align with the requirement for a fully managed solution. Amazon S3 (Option D) is an object storage service that does not provide file system semantics or native SMB access. new: waiting...

213. Question #250A 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?

- 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.

答案: D

解析: To meet the requirement of capturing VPC Flow Logs and managing their storage lifecycle, the solutions architect should use Amazon S3 as the target for the logs (Option D). By enabling an S3 Lifecycle policy, the logs can be transitioned to S3 Standard-Infrequent Access (S3

Standard-IA) after 90 days. This transition optimizes storage costs by moving the logs to a storage class designed for infrequent access while still allowing for intermittent access when needed. This approach is more cost-effective and aligned with the access pattern described compared to the other options, such as using CloudWatch or Kinesis, which do not offer the same lifecycle management and cost optimization for long-term storage, or using CloudTrail without the appropriate lifecycle management on S3.

解析: To meet the requirement of capturing VPC Flow Logs and managing their storage lifecycle, the solutions architect should use Amazon S3 as the target for the logs (Option D). By enabling an S3 Lifecycle policy, the logs can be transitioned to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days. This transition optimizes storage costs by moving the logs to a storage class designed for infrequent access while still allowing for intermittent access when needed. This approach is more cost-effective and aligned with the access pattern described compared to the other options, such as using CloudWatch or Kinesis, which do not offer the same lifecycle management and cost optimization for long-term storage, or using CloudTrail without the appropriate lifecycle management on S3.

214. Question #251An 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?

- 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.

答案：B

解析：To allow an EC2 instance in a private subnet to access the internet for security updates without providing direct internet access, a solutions architect should create a NAT gateway (Option B). The NAT gateway should be placed in a public subnet and the route table for the private subnet should be configured to use the NAT gateway as its default route. This setup enables the EC2 instance to access the internet while remaining in a private subnet, maintaining security and control over internet access.

解析：To allow an EC2 instance in a private subnet to access the internet for security updates without providing direct internet access, a solutions architect should create a NAT gateway (Option B). The NAT gateway should be placed in a public subnet and the route table for the private subnet should be configured to use the NAT gateway as its default route. This setup enables the EC2 instance to access the internet while remaining in a private subnet, maintaining security and control over internet access.

215. Question #252A 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?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier Deep Archive
- D. AWS Backup

答案：A

解析: Amazon Elastic File System (Amazon EFS) (Option A) is the solution that meets the requirements. EFS is a scalable file storage service for use with AWS Cloud services that can be accessed by multiple EC2 instances simultaneously. It provides built-in redundancy and the ability to grow over time, making it suitable for storing important company assets like client case files.

解析: Amazon Elastic File System (Amazon EFS) (Option A) is the solution that meets the requirements. EFS is a scalable file storage service for use with AWS Cloud services that can be accessed by multiple EC2 instances simultaneously. It provides built-in redundancy and the ability to grow over time, making it suitable for storing important company assets like client case files.

216. Question #253A 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?

Policy 1

```
{  
    "Version": "2012-10-17", "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iam:Get*",  
                "iam>List*",  
                "kms>List*",  
                "ec2:*",  
                "ds:*",  
                "logs:Get*",  
                "logs:Describe*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Policy 2

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ds:Delete*",  
            "Resource": "*"  
        }  
    ]  
}
```

- A. Deleting IAM users
- B. Deleting directories
- C. Deleting Amazon EC2 instances
- D. Deleting logs from Amazon CloudWatch Logs

答案: C

解析: The cloud engineer, being part of an IAM group with attached policies, will be able to perform actions permitted by the policies. If the policies grant permissions to delete Amazon EC2 instances (Option C), then the engineer will be able to do so. The other options, such as deleting IAM users (Option A), directories (Option B), or logs from Amazon CloudWatch Logs (Option D), are not directly related to EC2 instance management and would require specific permissions within the IAM policies to be allowed.

解析: The cloud engineer, being part of an IAM group with attached policies, will be able to perform actions permitted by the policies. If

the policies grant permissions to delete Amazon EC2 instances (Option C), then the engineer will be able to do so. The other options, such as deleting IAM users (Option A), directories (Option B), or logs from Amazon CloudWatch Logs (Option D), are not directly related to EC2 instance management and would require specific permissions within the IAM policies to be allowed.

217. Question #254A 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?

- 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.

答案：B

解析：To apply the principle of least privilege, the solutions architect should create security group rules using the security group ID as the source or destination (Option B). This allows for precise control over which resources can communicate with each other, ensuring that only the necessary traffic is allowed. Using instance IDs (Option A), VPC CIDR blocks (Option C), or subnet CIDR blocks (Option D) would be less restrictive and could potentially allow broader access than is necessary, which is not in line with the principle of least privilege.

解析：To apply the principle of least privilege, the solutions architect should create security group rules using the security group ID as the source or destination (Option B). This allows for precise control over which resources can communicate with each other, ensuring that only the necessary traffic is allowed. Using instance IDs (Option A), VPC CIDR

blocks (Option C), or subnet CIDR blocks (Option D) would be less restrictive and could potentially allow broader access than is necessary, which is not in line with the principle of least privilege.

218. Question #255A 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?

- 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.

答案: D

解析: To prevent the creation of multiple orders due to timeouts and retries during the checkout process, the solutions architect should use an Amazon SQS FIFO queue (Option D). By storing the order in the database and then sending a message with the order number to an SQS FIFO queue, the system can ensure that messages (and thus orders) are processed exactly once. The payment service can then retrieve and process the order from the queue, and the message can be deleted after successful processing to prevent duplicate orders. This approach avoids the issues that might arise with Kinesis Data Firehose (Option A), which is more

suited for streaming data scenarios, or AWS CloudTrail and Lambda (Option B), which are not designed for managing transactional order processing. Amazon SNS (Option C) does not guarantee message ordering or deduplication, making it less suitable for this requirement.

解析: To prevent the creation of multiple orders due to timeouts and retries during the checkout process, the solutions architect should use an Amazon SQS FIFO queue (Option D). By storing the order in the database and then sending a message with the order number to an SQS FIFO queue, the system can ensure that messages (and thus orders) are processed exactly once. The payment service can then retrieve and process the order from the queue, and the message can be deleted after successful processing to prevent duplicate orders. This approach avoids the issues that might arise with Kinesis Data Firehose (Option A), which is more suited for streaming data scenarios, or AWS CloudTrail and Lambda (Option B), which are not designed for managing transactional order processing. Amazon SNS (Option C) does not guarantee message ordering or deduplication, making it less suitable for this requirement.

219. Question #257A 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?

- 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.

答案：A

解析：To meet the requirements of reporting EC2 Auto Scaling events without affecting the speed of EC2 instance launches, the company should use an Amazon CloudWatch metric stream (Option A). This service can capture metrics and send them to Amazon Kinesis Data Firehose, which is a fully managed service for real-time streaming data ingestion. From there, the data can be stored in Amazon S3. This serverless approach ensures that the data transfer and storage process is efficient and does not interfere with the EC2 instance launch process.

解析：To meet the requirements of reporting EC2 Auto Scaling events without affecting the speed of EC2 instance launches, the company should use an Amazon CloudWatch metric stream (Option A). This service can capture metrics and send them to Amazon Kinesis Data Firehose, which is a fully managed service for real-time streaming data ingestion. From there, the data can be stored in Amazon S3. This serverless approach ensures that the data transfer and storage process is efficient and does not interfere with the EC2 instance launch process.

220. Question #258A 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?

- 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.

答案: D

解析: The solution that meets the requirements with the least operational overhead is to create an AWS Glue ETL job (Option D). AWS Glue is a fully managed ETL service that can automatically handle the conversion of .csv files to Parquet format and is triggered by S3 PUT events via an AWS Lambda function. This serverless approach reduces the need for manual intervention and eliminates the need to manage the underlying infrastructure.

解析: The solution that meets the requirements with the least operational overhead is to create an AWS Glue ETL job (Option D). AWS Glue is a fully managed ETL service that can automatically handle the conversion of .csv files to Parquet format and is triggered by S3 PUT events via an AWS Lambda function. This serverless approach reduces the need for manual intervention and eliminates the need to manage the underlying infrastructure.

221. Question #259A 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?

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.

答案：A

解析：To meet the data retention policy requirements for Amazon RDS DB instances, the solutions architect should recommend using AWS Backup (Option A). AWS Backup allows the creation of a backup plan with a daily schedule for RDS backups and can be configured to retain backups for a specified period, in this case, 2 years. This solution ensures that the backups are consistent, restorable, and meet the specified retention policy.

解析：To meet the data retention policy requirements for Amazon RDS DB instances, the solutions architect should recommend using AWS Backup (Option A). AWS Backup allows the creation of a backup plan with a daily schedule for RDS backups and can be configured to retain backups for a specified period, in this case, 2 years. This solution ensures that the backups are consistent, restorable, and meet the specified retention policy.

222. Question #260A 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?

- 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.

答案: D

解析: To ensure that the on-premises Active Directory groups continue to restrict access to the Amazon FSx for Windows File Server SMB shares after the move to AWS, the company should join the file system to the Active Directory (Option D). This allows the use of existing Active Directory groups and permissions, providing a seamless transition and maintaining compliance with the company's security policies.

解析: To ensure that the on-premises Active Directory groups continue to restrict access to the Amazon FSx for Windows File Server SMB shares after the move to AWS, the company should join the file system to the Active Directory (Option D). This allows the use of existing Active Directory groups and permissions, providing a seamless transition and maintaining compliance with the company's security policies.

223. Question #262A 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?

- 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.

答案：A

解析：The most cost-effective solution to provide the application's EC2 instances with access to the ElastiCache cluster is to create a peering connection between the VPCs (Option A). VPC peering allows the two VPCs to communicate as if they are part of the same network without the need for a central routing VPC (which would be the case with a Transit VPC in Option B). This eliminates additional costs and complexity. Adding a route table entry for the peering connection and configuring the security groups to allow inbound connections from the respective security groups completes the setup for secure and direct communication between the application and the cache cluster.

解析：The most cost-effective solution to provide the application's EC2 instances with access to the ElastiCache cluster is to create a peering connection between the VPCs (Option A). VPC peering allows the two VPCs to communicate as if they are part of the same network without the need for a central routing VPC (which would be the case with a Transit VPC in Option B). This eliminates additional costs and complexity. Adding a route table entry for the peering connection and configuring the security groups to allow inbound connections from the respective security groups completes the setup for secure and direct communication between the application and the cache cluster.

224. Question #264A 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?

- 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.

答案: D

解析: To overcome timeout errors caused by DNS queries returning IP addresses of unhealthy instances, a solutions architect should implement an Application Load Balancer (ALB) with a health check in front of the EC2 instances (Option D). By **routing traffic to the ALB from Route 53, the ALB can perform health checks on the instances and route traffic only to healthy instances.** This ensures that users are not directed to instances that are experiencing issues, thus preventing timeout errors.

解析: To overcome timeout errors caused by DNS queries returning IP addresses of unhealthy instances, a solutions architect should implement an Application Load Balancer (ALB) with a health check in front of the EC2 instances (Option D). By **routing traffic to the ALB from Route 53, the ALB can perform health checks on the instances and route traffic only to healthy instances.** This ensures that users are not directed to instances that are experiencing issues, thus preventing timeout errors.

225. Question #265A 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?

- 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.

答案：C

解析：The most secure and highly available solution for delivering HTTPS content with the least delivery time is to configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets (Option C). By using an ALB in private subnets, the EC2 instances are not directly accessible from the public internet, which enhances security. Configuring Amazon CloudFront to deliver content using the public ALB as the origin allows the content to be cached and delivered from the edge locations, minimizing the delivery time and ensuring high availability.

解析：The most secure and highly available solution for delivering HTTPS content with the least delivery time is to configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets (Option C). By using an ALB in private subnets, the EC2 instances are not directly accessible from the public internet, which enhances security. Configuring Amazon CloudFront to deliver content using the public ALB as the origin allows the content to be cached and delivered from the edge locations, minimizing the delivery time and ensuring high availability.

226. Question #266A 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?

- 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.

答案：A

解析：To monitor the health of the gaming application and redirect traffic to healthy endpoints across different AWS Regions, the solutions architect should configure an accelerator in AWS Global Accelerator (Option A). By adding a listener for the application's port and attaching it to a Regional endpoint in each Region, then adding the ALB as the endpoint, Global Accelerator can effectively route player traffic to the nearest healthy endpoint. This ensures low latency and a good user experience by directing traffic to the optimal endpoint based on health checks and geographic location.

解析：To monitor the health of the gaming application and redirect traffic to healthy endpoints across different AWS Regions, the solutions architect should configure an accelerator in AWS Global Accelerator

(Option A). By adding a listener for the application's port and attaching it to a Regional endpoint in each Region, then adding the ALB as the endpoint, Global Accelerator can effectively route player traffic to the nearest healthy endpoint. This ensures low latency and a good user experience by directing traffic to the optimal endpoint based on health checks and geographic location.

227. Question #267A 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?

- 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.

答案: D

解析: The solution that meets the requirements with the least operational overhead is to create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3 and create an Amazon Kinesis Data Analytics application to analyze the data (Option D). Kinesis Data Firehose can automatically encrypt the data as it is ingested and store it in S3 in the specified Parquet format. It can also directly invoke a Kinesis Data Analytics application for near-real-time data analysis, eliminating the need for additional services like AWS Lambda or an EMR cluster, which

would increase operational overhead.

解析: The solution that meets the requirements with the least operational overhead is to create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3 and create an Amazon Kinesis Data Analytics application to analyze the data (Option D). Kinesis Data Firehose can automatically encrypt the data as it is ingested and store it in S3 in the specified Parquet format. It can also directly invoke a Kinesis Data Analytics application for near-real-time data analysis, eliminating the need for additional services like AWS Lambda or an EMR cluster, which would increase operational overhead.

228. Question #268A **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?

- 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.

答案: A

解析: old (B) --> new (A) old: To improve the user experience with minimal changes to the application's architecture, the solutions architect should use RDS Proxy between the application and the database (Option B). RDS Proxy can help manage database connections, providing a more efficient and scalable solution for read operations. It can also improve the handling of database load by automatically distributing connections across multiple database instances. new: waiting...

解析: old (B) --> new (A) old: To improve the user experience with minimal changes to the application's architecture, the solutions architect should use RDS Proxy between the application and the database

(Option B). RDS Proxy can help manage database connections, providing a more efficient and scalable solution for read operations. It can also improve the handling of database load by automatically distributing connections across multiple database instances. new: waiting...

229. Question #269 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?

- 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.

答案: C

解析: To address the performance degradation caused by an increase in read-only SQL queries, the solutions architect should recommend creating a read replica of the primary database (Option C). This allows the read queries to be offloaded from the primary database to the read replica, which can help maintain performance for the main application while providing the necessary data for business analysts. This solution requires minimal changes to the existing web application, as it leverages the existing database infrastructure.

解析: To address the performance degradation caused by an increase in read-only SQL queries, the solutions architect should recommend creating a read replica of the primary database (Option C). This allows the read queries to be offloaded from the primary database to the read replica, which can help maintain performance for the main application while providing the necessary data for business analysts. This solution

requires minimal changes to the existing web application, as it leverages the existing database infrastructure.

230. Question #270A 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?

- 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.

答案: A

解析: To ensure that data is encrypted at rest before it is uploaded to Amazon S3 buckets, the solutions architect should use client-side encryption (Option A). This approach allows data to be encrypted before it leaves the sender's environment, meeting the requirement that data be encrypted prior to uploading. Additionally, to encrypt data in transit, the architect should ensure that data is transferred over secure protocols such as HTTPS.

解析: To ensure that data is encrypted at rest before it is uploaded to Amazon S3 buckets, the solutions architect should use client-side encryption (Option A). This approach allows data to be encrypted before it leaves the sender's environment, meeting the requirement that data be encrypted prior to uploading. Additionally, to encrypt data in transit, the architect should ensure that data is transferred over secure protocols such as HTTPS.

231. Question #271A 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 to find 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?

- 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.

答案：C

解析：To ensure that the desired EC2 capacity is reached quickly for a nightly batch processing job and to allow the Auto Scaling group to scale down after the job is complete, the solutions architect should configure scheduled scaling (Option C). Scheduled scaling allows for the planned increase and decrease of capacity at specific times, which is ideal for predictable workloads with fixed schedules, such as nightly batch jobs.

解析：To ensure that the desired EC2 capacity is reached quickly for a nightly batch processing job and to allow the Auto Scaling group to scale down after the job is complete, the solutions architect should configure scheduled scaling (Option C). Scheduled scaling allows for the planned increase and decrease of capacity at specific times, which is ideal for predictable workloads with fixed schedules, such as nightly batch jobs.

232. Question #272A 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?

- 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.

答案：B

解析：To serve requests quickly and efficiently for users around the world without recreating the existing architecture in multiple Regions, the solutions architect should configure an Amazon CloudFront distribution with the ALB as the origin (Option B). By setting the cache behavior settings in CloudFront to cache based on the Accept-Language request header, the website can serve different language versions of content to users based on their language preferences, reducing latency and improving the user experience.

解析：To serve requests quickly and efficiently for users around the world without recreating the existing architecture in multiple Regions, the solutions architect should configure an Amazon CloudFront distribution with the ALB as the origin (Option B). By setting the cache behavior settings in CloudFront to cache based on the Accept-Language request header, the website can serve different language versions of content to users based on their language preferences, reducing latency and improving the user experience.

233. Question #273A 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 (RT0)?

- 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.

答案：B

解析：To meet the requirements of having the database up to date with the least possible latency and a low RT0, the solutions architect should use an Amazon Aurora global database with a warm standby deployment (Option B). This setup allows for a global database that is continuously updated and can quickly be promoted to handle traffic in the event of a disaster. The warm standby maintains a high level of data replication and is designed to minimize RT0, making it suitable for disaster recovery needs.

解析：To meet the requirements of having the database up to date with the least possible latency and a low RT0, the solutions architect should use an Amazon Aurora global database with a warm standby deployment (Option B). This setup allows for a global database that is continuously updated and can quickly be promoted to handle traffic in the event of a disaster. The warm standby maintains a high level of data replication and is designed to minimize RT0, making it suitable for disaster recovery needs.

234. Question #274A 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 (RT0) 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?

- 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.

答案：B

解析：The most operationally efficient way to implement a DR solution with an RT0 of less than 4 hours and minimal resource usage is to create Amazon Machine Images (AMIs) of the EC2 instances and use AWS CloudFormation to automate the infrastructure deployment in a secondary AWS Region (Option B). This approach allows for a DR setup that can be quickly activated with CloudFormation templates, which are designed to provision and configure AWS resources consistently and quickly. This method requires fewer resources during normal operations compared to keeping instances active (Options C and D) and is more efficient than using Lambda and custom scripts (Option A).

解析：The most operationally efficient way to implement a DR solution with an RT0 of less than 4 hours and minimal resource usage is to create Amazon Machine Images (AMIs) of the EC2 instances and use AWS CloudFormation to automate the infrastructure deployment in a secondary AWS Region (Option B). This approach allows for a DR setup that can be quickly activated with CloudFormation templates, which are designed to provision and configure AWS resources consistently and quickly. This method requires fewer resources during normal operations compared to keeping instances active (Options C and D) and is more efficient than using Lambda and custom scripts (Option A).

235. Question #275A 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?

- 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.

答案：C

解析：To address the staff complaints about slow application performance at the beginning of the workday while keeping costs to a minimum, the best solution is to implement a scheduled scaling action. Here's how to change the scaling approach:

- 1. **Implement a Scheduled Action** – Create a scheduled scaling action in Amazon EC2 Auto Scaling. – Set the action to increase the desired capacity shortly before the office opens. – This ensures that the application has enough instances to handle the morning workload.
- 2. **Configure the Scheduled Action** – Set the desired capacity to a value higher than 2 but lower than 20. – For example, you might set it to 10 or 15 instances, depending on your typical morning workload. – Schedule this action to occur about 30 minutes before the office opens.
- 3. **Maintain Dynamic Scaling** – Keep your existing dynamic scaling policies in place. – These will allow the Auto Scaling group to adjust capacity throughout the day based on demand.
- 4. **Fine-tune Scaling Policies** – Review and adjust your scaling policies to ensure they respond quickly to increased load. – Consider lowering CPU thresholds for scale-out actions. – Decrease cooldown periods to allow faster scaling.
- 5. **Monitor and Adjust** – Use Amazon CloudWatch to monitor application performance and instance

utilization. – Adjust the scheduled action and dynamic scaling policies based on observed patterns. By implementing this solution, you'll have enough capacity to handle the morning rush while still allowing for cost-effective scaling throughout the day. The scheduled action ensures a smoother start to the workday, and the dynamic scaling policies continue to optimize resource usage and costs as demand fluctuates. Remember to test these changes in a non-production environment first and monitor the impact on both performance and costs. Regularly review and adjust your Auto Scaling settings to ensure they continue to meet your needs as usage patterns may change over time.

Sources [1] [Amazon EC2 Auto Scaling Features]

(<https://aws.amazon.com/ec2/autoscaling/features/>) [3] [What is Amazon EC2 Auto Scaling? – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>) [6] [Auto Scaling groups – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>)

解析: To address the staff complaints about slow application performance at the beginning of the workday while keeping costs to a minimum, the best solution is to implement a scheduled scaling action. Here's how to change the scaling approach:

1. **Implement a Scheduled Action** – Create a scheduled scaling action in Amazon EC2 Auto Scaling. – Set the action to increase the desired capacity shortly before the office opens. – This ensures that the application has enough instances to handle the morning workload.
2. **Configure the Scheduled Action** – Set the desired capacity to a value higher than 2 but lower than 20. – For example, you might set it to 10 or 15 instances, depending on your typical morning workload. – Schedule this action to occur about 30 minutes before the office opens.
3. **Maintain Dynamic Scaling** – Keep your existing dynamic scaling policies in place. – These will allow the Auto Scaling group to adjust capacity throughout the day based on demand.
4. **Fine-tune Scaling Policies** – Review and adjust your scaling policies to ensure they respond quickly to increased load. – Consider lowering CPU thresholds for scale-out actions. – Decrease cooldown periods to allow faster scaling.
5. **Monitor and Adjust** –

Use Amazon CloudWatch to monitor application performance and instance utilization.

- Adjust the scheduled action and dynamic scaling policies based on observed patterns. By implementing this solution, you'll have enough capacity to handle the morning rush while still allowing for cost-effective scaling throughout the day. The scheduled action ensures a smoother start to the workday, and the dynamic scaling policies continue to optimize resource usage and costs as demand fluctuates. Remember to test these changes in a non-production environment first and monitor the impact on both performance and costs.

Regularly review and adjust your Auto Scaling settings to ensure they continue to meet your needs as usage patterns may change over time.

Sources [1] [Amazon EC2 Auto Scaling Features]

(<https://aws.amazon.com/ec2/autoscaling/features/>) [3] [What is Amazon EC2 Auto Scaling? – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>) [6] [Auto Scaling groups – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>)

236. Question #277A 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**?

- 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.

答案：D

解析：The most cost-effective storage solution for storing video content, especially when dealing with large amounts of data, is to use Amazon S3. S3 is a highly scalable and durable object storage service that is designed to keep costs low for long-term storage. By using S3, the company can take advantage of its low storage costs. D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon EBS volume attached to the server for processing. This approach allows for the video content to be stored cost-effectively in S3 and then temporarily transferred to an EBS volume for processing by the EC2 instances. EBS provides high performance for processing the videos, while S3 keeps the storage costs down. After processing, the videos can be returned to S3 for long-term storage or further distribution. Options A and B are less cost-effective because AWS Storage Gateway is typically used for hybrid storage solutions that connect on-premises infrastructure to AWS cloud storage, which may not be as efficient for purely cloud-based processing workflows. Option C suggests using Amazon EFS, which is a file system service that is more expensive than S3 for storing large volumes of data, especially when the data does not need the high performance and file system interface that EFS provides.

解析：The most cost-effective storage solution for storing video content, especially when dealing with large amounts of data, is to use Amazon S3. S3 is a highly scalable and durable object storage service that is designed to keep costs low for long-term storage. By using S3, the company can take advantage of its low storage costs. D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon EBS volume attached to the server for processing. This approach allows for the video content to be stored cost-effectively in S3 and then temporarily transferred to an EBS volume for processing by the EC2 instances. EBS provides high performance for processing the videos, while S3 keeps the storage costs down. After processing, the videos can be returned to S3 for long-term storage or further distribution. Options A and B are less cost-effective because AWS Storage Gateway is typically used for hybrid storage solutions that connect on-premises infrastructure

to AWS cloud storage, which may not be as efficient for purely cloud-based processing workflows. Option C suggests using Amazon EFS, which is a file system service that is more expensive than S3 for storing large volumes of data, especially when the data does not need the high performance and file system interface that EFS provides.

237. Question #279A 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?

- 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.

答案：A

解析：To meet the compliance requirements for database backups, a solutions architect should: 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. AWS Backup is a service designed for backing up AWS resources. It can be scheduled to take regular backups and can be configured with lifecycle policies that automatically transition backups to cheaper storage options after a certain period, in this case, to Amazon S3 Glacier after 6 months. The retention policy can also be set to keep backups for the required 7 years, ensuring that the backups are available for the necessary duration and are then deleted in accordance with the compliance policy. Option B requires manual intervention to transition backups to cold storage and to delete them after 7 years, which is not as automated or compliant with the requirements as option A. Option C involves custom scripting and setup with EventBridge, which adds complexity and potential for error. Option D is similar to option C but uses the AWS CLI instead of the SDK, and it also requires custom scripting and setup with EventBridge, making it less ideal than the automated and integrated solution provided by AWS Backup in option A.

解析: To meet the compliance requirements for database backups, a solutions architect should: 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. AWS Backup is a service designed for backing up AWS resources. It can be scheduled to take regular backups and can be configured with lifecycle policies that automatically transition backups to cheaper storage options after a certain period, in this case, to Amazon S3 Glacier after 6 months. The retention policy can also be set to keep backups for the required 7 years, ensuring that the backups are available for the necessary duration and are then deleted in accordance with the compliance policy. Option B requires manual intervention to transition backups to cold storage and to delete them after 7 years, which is not as automated or compliant with the requirements as option A. Option C involves custom scripting and setup with EventBridge, which adds complexity and potential for error. Option D is similar to option C but uses the AWS CLI instead of the SDK,

and it also requires custom scripting and setup with EventBridge, making it less ideal than the automated and integrated solution provided by AWS Backup in option A.

238. Question #280A 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?

- 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.

答案: B

解析: To analyze logs and build visualizations, a solutions architect should:

- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight. **Amazon Athena is an interactive query service that allows users to analyze data directly in S3 using standard SQL. Once the data is analyzed, the results can be visualized using Amazon QuickSight, a business analytics service that can create visualizations, reports, and dashboards.** QuickSight integrates well with Athena and provides an easy way to create interactive visuals that can help in understanding the log data.

Option A is incorrect because AWS Glue is a data cataloging and ETL (extract, transform, load) service, not a visualization tool. Option C is incorrect because it suggests using Amazon DynamoDB, which is a NoSQL database service, not a tool for analyzing log files stored in S3. Option D is incorrect for the same reason as option C regarding DynamoDB, and also because QuickSight is a more suitable tool for visualization than Glue.

解析: To analyze logs and build visualizations, a solutions architect should:
B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight. Amazon Athena is an interactive query service that allows users to analyze data directly in S3 using standard SQL. Once the data is analyzed, the results can be visualized using Amazon QuickSight, a business analytics service that can create visualizations, reports, and dashboards. QuickSight integrates well with Athena and provides an easy way to create interactive visuals that can help in understanding the log data.
Option A is incorrect because AWS Glue is a data cataloging and ETL (extract, transform, load) service, not a visualization tool. Option C is incorrect because it suggests using Amazon DynamoDB, which is a NoSQL database service, not a tool for analyzing log files stored in S3. Option D is incorrect for the same reason as option C regarding DynamoDB, and also because QuickSight is a more suitable tool for visualization than Glue.

239. Question #281A 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?

- 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.

答案: A

解析: To meet the requirement of a recovery point objective (RPO) of less than 1 second for production databases, a solutions architect should:
A. Enable a Multi-AZ deployment for the DB instance. Multi-AZ deployment in Amazon RDS provides a high level of fault tolerance and disaster recovery by automatically replicating the database to a standby instance in a

different Availability Zone. This process ensures that the standby instance is always up-to-date with the primary instance, which allows for a very low RPO and minimal data loss in the event of a failure. Option B, enabling auto scaling, does not address the RPO requirement as it is related to scaling resources to meet demand rather than data replication for recovery purposes. Option C, creating read replicas, can improve read performance and provide some level of disaster recovery but does not maintain the same level of data replication as Multi-AZ deployment. Option D, using AWS DMS with CDC, is more relevant for data migration tasks rather than providing a low RPO for disaster recovery.

解析: To meet the requirement of a recovery point objective (RPO) of less than 1 second for production databases, a solutions architect should: A. Enable a Multi-AZ deployment for the DB instance. Multi-AZ deployment in Amazon RDS provides a high level of fault tolerance and disaster recovery by automatically replicating the database to a standby instance in a different Availability Zone. This process ensures that the standby instance is always up-to-date with the primary instance, which allows for a very low RPO and minimal data loss in the event of a failure. Option B, enabling auto scaling, does not address the RPO requirement as it is related to scaling resources to meet demand rather than data replication for recovery purposes. Option C, creating read replicas, can improve read performance and provide some level of disaster recovery but does not maintain the same level of data replication as Multi-AZ deployment. Option D, using AWS DMS with CDC, is more relevant for data migration tasks rather than providing a low RPO for disaster recovery.

240. Question #282A 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?

- 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.

答案：B

解析：To implement security measures that restrict inbound traffic from the ALB to the EC2 instances and prevent access from any other source, a solutions architect should: B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. Security groups act as a virtual firewall for EC2 instances and can be configured with rules that allow or deny traffic based on the source. By setting up the security group to only allow traffic from the ALB's security group, the EC2 instances will only accept traffic that is routed through the ALB, effectively blocking any direct access from the internet or other unauthorized sources. Option A is incorrect because routing traffic from the internet to the private IP addresses would expose the EC2 instances to the public, which is not secure. Option C is incorrect because moving the EC2 instances to the public subnet and assigning Elastic IP addresses would also expose them to the internet, which is against the requirement to keep them in a private subnet. Option D is incorrect because allowing any TCP traffic on any port through the ALB's security group would not provide the necessary restrictions and would open up the application to potential security threats.

解析：To implement security measures that restrict inbound traffic from the ALB to the EC2 instances and prevent access from any other source, a solutions architect should: B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. Security groups act as a virtual firewall for EC2 instances and can be configured with rules that allow or deny traffic based on the source. By setting up the security group to only allow traffic from the

ALB's security group, the EC2 instances will only accept traffic that is routed through the ALB, effectively blocking any direct access from the internet or other unauthorized sources. Option A is incorrect because routing traffic from the internet to the private IP addresses would expose the EC2 instances to the public, which is not secure. Option C is incorrect because moving the EC2 instances to the public subnet and assigning Elastic IP addresses would also expose them to the internet, which is against the requirement to keep them in a private subnet. Option D is incorrect because allowing any TCP traffic on any port through the ALB's security group would not provide the necessary restrictions and would open up the application to potential security threats.

241. Question #283A 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?

- 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.

答案: D

解析: To migrate the applications to AWS without making code changes and to address the data duplication and inefficient resource usage, a solutions architect should: 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. **Amazon FSx for NetApp ONTAP is a fully managed service that provides a highly available file system that supports both NFS and SMB protocols, which is suitable for Linux and Windows environments.** This service allows the simulation application to continue using NFS and the visualization application to use SMB, without the need for code changes. Additionally, FSx for NetApp ONTAP can be connected to the EC2 instances, providing a shared storage solution that eliminates the need for synchronizing two separate file systems. Option A is incorrect because AWS Lambda is not designed for persistent storage or sharing of large amounts of data between applications. Option B is incorrect because Amazon FSx File Gateway does not support SMB protocol, which is required by the Windows application. Option C is incorrect because Amazon SQS is a message queuing service and not a file system, which does not meet the requirements for shared file storage between the Linux and Windows applications.

解析: To migrate the applications to AWS without making code changes and to address the data duplication and inefficient resource usage, a solutions architect should: 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. **Amazon FSx for NetApp ONTAP is a fully managed service that provides a highly available file system that supports both NFS and SMB protocols, which is suitable for Linux and Windows environments.** This service allows the simulation application to continue using NFS and the visualization application to use SMB, without the need for code changes. Additionally, FSx for NetApp ONTAP can be connected to the EC2 instances, providing a shared storage solution that eliminates the need for synchronizing two separate file systems. Option A is incorrect because AWS Lambda is not designed for persistent storage or sharing of large amounts of data

between applications. Option B is incorrect because Amazon FSx File Gateway does not support SMB protocol, which is required by the Windows application. Option C is incorrect because Amazon SQS is a message queuing service and not a file system, which does not meet the requirements for shared file storage between the Linux and Windows applications.

242. Question #284As 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?

- 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).

答案：B

解析：To obtain a report of AWS billed items listed by user for budget planning purposes, a solutions architect should: B. Create a report in Cost Explorer and download the report. **AWS Cost Explorer provides a way to visualize and understand your AWS costs and usage.** It allows you to create reports that can be filtered by various dimensions, including user, which makes it possible to generate a report that lists billed items by user. These reports can be downloaded for further analysis or used to create department budgets. Option A, running a query with Amazon Athena, would require setting up additional infrastructure and is not as straightforward for generating reports based on billing data. Option C, downloading the bill from the billing dashboard, does not provide the granularity of listing billed items by user. Option D, modifying a cost budget in AWS Budgets to alert with Amazon SES, is not designed for generating detailed billing reports and would not meet the requirement of listing billed items by user.

解析: To obtain a report of AWS billed items listed by user for budget planning purposes, a solutions architect should: B. Create a report in Cost Explorer and download the report. AWS Cost Explorer provides a way to visualize and understand your AWS costs and usage. It allows you to create reports that can be filtered by various dimensions, including user, which makes it possible to generate a report that lists billed items by user. These reports can be downloaded for further analysis or used to create department budgets. Option A, running a query with Amazon Athena, would require setting up additional infrastructure and is not as straightforward for generating reports based on billing data. Option C, downloading the bill from the billing dashboard, does not provide the granularity of listing billed items by user. Option D, modifying a cost budget in AWS Budgets to alert with Amazon SES, is not designed for generating detailed billing reports and would not meet the requirement of listing billed items by user.

243. Question #285A 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?
- 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.

答案：B

解析：For a static website with low traffic that requires a contact form with server-side components, the most cost-effective solution is: B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon SES. This setup is serverless, which means there is no need to provision or manage any servers. API Gateway handles the HTTP requests from the contact form, while Lambda runs the code to process the form data and SES sends the email. This solution scales automatically with the number of form submissions and is cost-effective for low volumes of traffic. Option A, hosting a dynamic contact form page in Amazon ECS, would be more expensive due to the management and operation of container instances. Option C, deploying Amazon Lightsail, and Option D, creating an EC2 instance with a LAMP stack, both involve managing servers, which is not necessary for the described use case and would incur additional costs.

解析：For a static website with low traffic that requires a contact form with server-side components, the most cost-effective solution is: B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon SES. This setup is serverless, which means there is no need to provision or manage any servers. API Gateway handles the HTTP requests from the contact form, while Lambda runs the code to process the form data and SES sends the email. This solution scales automatically with the number of form submissions and is cost-effective for low volumes of traffic. Option A, hosting a dynamic contact form page in Amazon ECS, would be more expensive due to the management and operation of container instances. Option C, deploying Amazon Lightsail, and Option D, creating an EC2 instance with a LAMP stack, both involve managing servers, which is not necessary for the described use case and would incur additional costs.

244. Question #286A 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?

- 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.

答案: C

解析: When updates to a static website hosted on Amazon S3 do not reflect on the live site served by Amazon CloudFront, it's often because the updated content is not being fetched from the origin S3 bucket due to caching. To ensure that the visitors see the latest version of the website, the solutions architect should: C. Invalidate the CloudFront cache. Invalidating the cache in CloudFront will force the CDN to fetch the latest content from the S3 bucket the next time a user requests the page. This ensures that the updates made to the website's Git repository and subsequently deployed to S3 are displayed to the users. Option A, adding an Application Load Balancer, is not relevant to the issue of updating content on a static website. Option B, adding Amazon ElastiCache, is related to improving the performance of dynamic components by caching data, but it does not address the problem of reflecting updates made to a static website. Option D, using AWS Certificate Manager to validate the SSL certificate, is important for security but does not affect the content deployment or caching behavior.

解析: When updates to a static website hosted on Amazon S3 do not reflect on the live site served by Amazon CloudFront, it's often because the updated content is not being fetched from the origin S3 bucket due to caching. To ensure that the visitors see the latest version of the website, the solutions architect should: C. Invalidate the CloudFront

cache. Invalidating the cache in CloudFront will force the CDN to fetch the latest content from the S3 bucket the next time a user requests the page. This ensures that the updates made to the website's Git repository and subsequently deployed to S3 are displayed to the users. Option A, adding an Application Load Balancer, is not relevant to the issue of updating content on a static website. Option B, adding Amazon ElastiCache, is related to improving the performance of dynamic components by caching data, but it does not address the problem of reflecting updates made to a static website. Option D, using AWS Certificate Manager to validate the SSL certificate, is important for security but does not affect the content deployment or caching behavior.

245. Question #287A 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?

- 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.

答案：B

解析：To migrate a Windows-based application to AWS Cloud while using specific SQL Server features and sharing files between tiers, a solutions architect should: B. Host all three tiers on Amazon EC2 instances. Use

Amazon FSx for Windows File Server for file sharing between the tiers. Amazon FSx for Windows File Server is a fully managed service that provides a familiar and consistent file system experience compatible with Windows applications, making it suitable for hosting the application, business, and database tiers. It supports features like file sharing and integrates well with Windows-based workloads, meeting the requirements for sharing files between the application tiers. Option A is incorrect because Amazon FSx File Gateway is designed for caching frequently accessed files from S3, which is not the best fit for hosting file shares required by the application tiers. Option C is incorrect because Amazon EFS is a file system for Linux-based applications and does not support Windows file sharing protocols. Option D is incorrect because Amazon EBS is block storage and does not provide file system sharing capabilities.

解析: To migrate a Windows-based application to AWS Cloud while using specific SQL Server features and sharing files between tiers, a solutions architect should: B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers. Amazon FSx for Windows File Server is a fully managed service that provides a familiar and consistent file system experience compatible with Windows applications, making it suitable for hosting the application, business, and database tiers. It supports features like file sharing and integrates well with Windows-based workloads, meeting the requirements for sharing files between the application tiers. Option A is incorrect because Amazon FSx File Gateway is designed for caching frequently accessed files from S3, which is not the best fit for hosting file shares required by the application tiers. Option C is incorrect because Amazon EFS is a file system for Linux-based applications and does not support Windows file sharing protocols. Option D is incorrect because Amazon EBS is block storage and does not provide file system sharing capabilities.

246. Question #288A 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?

- 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.

答案: C

解析: To migrate Linux-based web servers to AWS without making any changes to the application and to provide access to a shared file store, a solutions architect should: C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers. Amazon EFS is a scalable file storage service for use with AWS Cloud services and on-premises resources. It provides a simple, scalable, and fully managed elastic NFS file system that can be mounted on multiple EC2 instances, making it ideal for shared access to files without application changes. Option A, using Amazon S3, is not suitable because S3 is an object storage service and not designed for use as a file system. Option B, configuring Amazon CloudFront, is a content delivery network solution and does not provide shared file storage. Option D, using Amazon EBS, is not appropriate because EBS volumes can only be attached to a single EC2 instance at a time, which does not meet the requirement for a shared file store accessible by multiple web servers.

解析: To migrate Linux-based web servers to AWS without making any changes to the application and to provide access to a shared file store, a solutions architect should: C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers. Amazon EFS is a scalable file storage service for use with AWS Cloud services and on-premises resources. It provides a simple, scalable, and fully managed elastic NFS file system that can be mounted on multiple EC2 instances, making it ideal for shared access to files without application changes. Option A, using Amazon S3, is not suitable because S3 is an object storage service and not designed for use as a file system. Option B, configuring Amazon CloudFront, is a content delivery network solution

and does not provide shared file storage. Option D, using Amazon EBS, is not appropriate because EBS volumes can only be attached to a single EC2 instance at a time, which does not meet the requirement for a shared file store accessible by multiple web servers.

247. Question #289A 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?**

- 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.

答案：B

解析：To grant an AWS Lambda function read access to an Amazon S3 bucket in the most secure manner, a solutions architect should: B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket. This approach adheres to the principle of least privilege, as the Lambda function will only have the permissions necessary to perform its intended function. By assigning an IAM role to the Lambda function, you can avoid embedding credentials within the function's code, which reduces the risk of accidental exposure or misuse. The IAM policy attached to the role can be scoped specifically to the S3 bucket in question, ensuring that the Lambda function has only the access required and no more. Option A, applying an S3 bucket policy, is less secure because it does not adhere to the principle of least privilege and could potentially grant more access than necessary. Option C, embedding access keys in the code, is not a secure practice as it risks exposing credentials. Option D, granting read access to all S3 buckets, is overly permissive and does not follow the principle of least privilege.

解析: To grant an AWS Lambda function read access to an Amazon S3 bucket in the most secure manner, a solutions architect should: B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket. This approach adheres to the principle of least privilege, as the Lambda function will only have the permissions necessary to perform its intended function. By assigning an IAM role to the Lambda function, you can avoid embedding credentials within the function's code, which reduces the risk of accidental exposure or misuse. The IAM policy attached to the role can be scoped specifically to the S3 bucket in question, ensuring that the Lambda function has only the access required and no more. Option A, applying an S3 bucket policy, is less secure because it does not adhere to the principle of least privilege and could potentially grant more access than necessary. Option C, embedding access keys in the code, is not a secure practice as it risks exposing credentials. Option D, granting read access to all S3 buckets, is overly permissive and does not follow the principle of least privilege.

248. Question #290A 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?

- 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

答案: C

解析: To optimize cost savings for a web application hosted on Amazon EC2 instances without making a long-term commitment, a solutions architect should recommend: C. A mix of On-Demand Instances and Spot Instances. This purchasing option allows the company to take advantage of the lower costs of Spot Instances while maintaining a baseline level of capacity with On-Demand Instances. Spot Instances can significantly reduce computing costs as they allow users to bid on spare EC2 capacity. By

combining this with On-Demand Instances, the company can ensure that it always has the required level of capacity to meet user demand while optimizing for cost. Option A, Dedicated Instances, are more expensive and typically used for compliance or when running licenses that require a physical dedicated infrastructure. Option B, On-Demand Instances only, does not provide any cost optimization benefits compared to a mix of instance types. Option D, a mix of On-Demand Instances and Reserved Instances, would require a long-term commitment, which the company wishes to avoid.

解析: To optimize cost savings for a web application hosted on Amazon EC2 instances without making a long-term commitment, a solutions architect should recommend: C. A mix of On-Demand Instances and Spot Instances. This purchasing option allows the company to take advantage of the lower costs of Spot Instances while maintaining a baseline level of capacity with On-Demand Instances. Spot Instances can significantly reduce computing costs as they allow users to bid on spare EC2 capacity. By combining this with On-Demand Instances, the company can ensure that it always has the required level of capacity to meet user demand while optimizing for cost. Option A, Dedicated Instances, are more expensive and typically used for compliance or when running licenses that require a physical dedicated infrastructure. Option B, On-Demand Instances only, does not provide any cost optimization benefits compared to a mix of instance types. Option D, a mix of On-Demand Instances and Reserved Instances, would require a long-term commitment, which the company wishes to avoid.

249. Question #293A 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?

- 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.

答案: D

解析: To replace an on-premises volume backup solution with an AWS-based solution that maintains local access to data, a solutions architect should: D. Use AWS Storage Gateway and configure a stored volume gateway. This option allows on-premises systems to connect to AWS-based storage volumes that are backed up to Amazon S3. The stored volume gateway retains the entire dataset on-premises and asynchronously backs up the data to AWS, ensuring that local access is maintained while the data is securely transferred and stored in the cloud. Option A, using AWS Snowball, is designed for data migration rather than ongoing backup solutions and does not maintain local access. Option B, AWS Snowball Edge, provides data transfer and edge computing capabilities but is not primarily designed for continuous backup solutions. Option C, a cached volume gateway, caches only frequently accessed data locally and is not suitable for maintaining local access to all data.

解析: To replace an on-premises volume backup solution with an AWS-based solution that maintains local access to data, a solutions architect should: D. Use AWS Storage Gateway and configure a stored volume gateway. This option allows on-premises systems to connect to AWS-based storage volumes that are backed up to Amazon S3. The stored volume gateway retains the entire dataset on-premises and asynchronously backs up the data to AWS, ensuring that local access is maintained while the data is

securely transferred and stored in the cloud. Option A, using AWS Snowball, is designed for data migration rather than ongoing backup solutions and does not maintain local access. Option B, AWS Snowball Edge, provides data transfer and edge computing capabilities but is not primarily designed for continuous backup solutions. Option C, a cached volume gateway, caches only frequently accessed data locally and is not suitable for maintaining local access to all data.

250. Question #294 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?

- 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.

答案：B

解析：To allow Amazon EC2 instances to access an Amazon S3 bucket without internet traversal, a solutions architect should: B. Set up a gateway VPC endpoint for Amazon S3 in the VPC. A VPC endpoint for S3 enables private communication between the VPC and S3 without exposing the traffic to the public internet. This is achieved by leveraging AWS PrivateLink, which provides a private connection between services without requiring an internet gateway, NAT device, or VPN. Option A, creating a private hosted zone with Amazon Route 53, is related to DNS management and does not address the requirement for private access to S3. Option C, configuring EC2 instances to use a NAT gateway, would route traffic over the internet, which is against the stated requirements. Option D, establishing a Site-to-Site VPN, is typically used for connecting to remote networks and not for private access to AWS services within the same AWS environment.

解析: To allow Amazon EC2 instances to access an Amazon S3 bucket without internet traversal, a solutions architect should: B. Set up a gateway VPC endpoint for Amazon S3 in the VPC. A VPC endpoint for S3 enables private communication between the VPC and S3 without exposing the traffic to the public internet. This is achieved by leveraging AWS PrivateLink, which provides a private connection between services without requiring an internet gateway, NAT device, or VPN. Option A, creating a private hosted zone with Amazon Route 53, is related to DNS management and does not address the requirement for private access to S3. Option C, configuring EC2 instances to use a NAT gateway, would route traffic over the internet, which is against the stated requirements. Option D, establishing a Site-to-Site VPN, is typically used for connecting to remote networks and not for private access to AWS services within the same AWS environment.

251. Question #295An 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?**

- 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.

答案: B

解析: To remove PII from customer data with the least operational overhead while allowing three applications to use the data, a solutions architect should: B. Store the data in an Amazon S3 bucket and use S3 Object Lambda to process and transform the data before returning it to the requesting application. S3 Object Lambda allows custom code to be executed每次从S3获取对象时，对数据进行处理，例如PII的自动删除或数据转换。这种方法避免了维护单独的数据集或代理应用程序层，从而降低了操作开销。 Option A, using a proxy application layer, would require additional development and maintenance overhead. Option C, storing transformed data in separate S3 buckets, and Option D, storing data in separate DynamoDB tables, would both require more operational overhead to maintain separate datasets and ensure consistency across them.

解析: To remove PII from customer data with the least operational overhead while allowing three applications to use the data, a solutions architect should: B. Store the data in an Amazon S3 bucket and use S3 Object Lambda to process and transform the data before returning it to the requesting application. S3 Object Lambda allows custom code to be executed每次从S3获取对象时，对数据进行处理，例如PII的自动删除或数据转换。这种方法避免了维护单独的数据集或代理应用程序层，从而降低了操作开销。 Option A, using a proxy application layer, would require additional development and maintenance overhead. Option C, storing transformed data in separate S3 buckets, and Option D, storing data in separate DynamoDB tables, would both require more operational overhead to maintain separate datasets and ensure consistency across them.

252. Question #296A 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?**

- A. 10.0.1.0/32

- B. 192.168.0.0/24
- C. 192.168.1.0/32
- D. 10.0.1.0/24**

答案: D

解析: When creating a new VPC to peer with an existing development VPC, the new VPC's CIDR block must not overlap with the CIDR block of the development VPC to avoid IP address conflicts. The smallest possible CIDR block that can be used while still being able to peer with the development VPC is /24, as this provides a unique IP range that is not within the 192.168.0.0/24 range of the development VPC. A. 10.0.1.0/32 is too small (a single IP address) and does not provide a range for multiple instances or services. B. 192.168.0.0/24 overlaps with the existing development VPC's CIDR block. C. 192.168.1.0/32 is also too small for the same reason as option A. D. 10.0.1.0/24 is the correct choice as it provides a unique and non-overlapping IP range that is suitable for the new VPC and allows for a VPC peering connection with the development VPC.

解析: When creating a new VPC to peer with an existing development VPC, the new VPC's CIDR block must not overlap with the CIDR block of the development VPC to avoid IP address conflicts. The smallest possible CIDR block that can be used while still being able to peer with the development VPC is /24, as this provides a unique IP range that is not within the 192.168.0.0/24 range of the development VPC. A. 10.0.1.0/32 is too small (a single IP address) and does not provide a range for multiple instances or services. B. 192.168.0.0/24 overlaps with the existing development VPC's CIDR block. C. 192.168.1.0/32 is also too small for the same reason as option A. D. 10.0.1.0/24 is the correct choice as it provides a unique and non-overlapping IP range that is suitable for the new VPC and allows for a VPC peering connection with the development VPC.

253. Question #297A 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?

- 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%.
- 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.

答案：B

解析：To automate the scalability of the application and optimize the cost while ensuring sufficient CPU resources during surges, a solutions architect should: B. Create an EC2 Auto Scaling group with a target tracking scaling policy based on the ASGAverageCPUUtilization metric. This configuration allows the Auto Scaling group to automatically adjust the number of instances based on the tracked CPU utilization metric. By setting the target value to 50%, the system will aim to maintain an average CPU utilization of 50% across all instances. This approach ensures that during low-traffic periods, the number of running instances can scale down to the minimum of 2 to save costs, and during high-traffic

periods (surges), it can scale up to the maximum of 6 instances to handle the increased load. Option A is not optimal because it suggests terminating instances when CPU utilization is low, which does not align with the goal of ensuring enough CPU resources during surges. Option C does not specify an auto-scaling policy based on CPU utilization, which is necessary for cost optimization and handling variable load. Option D relies on manual intervention to adjust the number of instances after receiving an email notification, which is not automated and does not ensure a timely response to changing CPU demands.

解析: To automate the scalability of the application and optimize the cost while ensuring sufficient CPU resources during surges, a solutions architect should: B. Create an EC2 Auto Scaling group with a target tracking scaling policy based on the ASGAverageCPUUtilization metric. This configuration allows the Auto Scaling group to automatically adjust the number of instances based on the tracked CPU utilization metric. By setting the target value to 50%, the system will aim to maintain an average CPU utilization of 50% across all instances. This approach ensures that during low-traffic periods, the number of running instances can scale down to the minimum of 2 to save costs, and during high-traffic periods (surges), it can scale up to the maximum of 6 instances to handle the increased load. Option A is not optimal because it suggests terminating instances when CPU utilization is low, which does not align with the goal of ensuring enough CPU resources during surges. Option C does not specify an auto-scaling policy based on CPU utilization, which is necessary for cost optimization and handling variable load. Option D relies on manual intervention to adjust the number of instances after receiving an email notification, which is not automated and does not ensure a timely response to changing CPU demands.

254. Question #298A 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**?

- 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.

答案: C

解析: To update the design and ensure high availability of the application, a solutions architect should: C. Provision a subnet in each Availability Zone and configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. This ensures that the application layer (EC2 instances) is spread across multiple Availability Zones, providing redundancy and fault tolerance. Additionally, configure the DB instance for Multi-AZ deployment, which automatically creates a synchronous standby replica of the DB instance in a different Availability Zone. This setup provides data redundancy, automatic failover, and eliminates the need for manual intervention in the event of a failure. Option A is incorrect because it does not specify the use of Multi-AZ deployment for the DB instance, which is necessary for high availability. Option B is incorrect because **AWS does not support subnets that span across multiple Availability Zones.** Option D is also incorrect for the same reason as option B regarding subnets and does not mention the need for Multi-AZ deployment for the DB instance.

解析: To update the design and ensure high availability of the application, a solutions architect should: C. Provision a subnet in each Availability Zone and configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. This ensures that the application layer (EC2 instances) is spread across multiple Availability Zones, providing redundancy and fault tolerance. Additionally, configure the DB instance for Multi-AZ deployment, which automatically creates a synchronous standby replica of the DB instance in a different Availability Zone. This setup provides data redundancy, automatic failover, and eliminates the need for manual intervention in the event of a failure. Option A is incorrect because it does not specify the use of Multi-AZ deployment for the DB instance, which is necessary for high availability. Option B is incorrect because AWS does not support subnets that span across multiple Availability Zones. Option D is also incorrect for the same reason as option B regarding subnets and does not mention the need for Multi-AZ deployment for the DB instance.

255. Question #299A 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?

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.

答案：B

解析：To meet the stringent performance requirements of sub-millisecond latencies and a minimum throughput of 6 Gbps, a solutions architect should: B. Create an Amazon S3 bucket to store the raw data and an Amazon FSx for Lustre file system that uses persistent SSD storage. Lustre is a high-performance file system designed for compute-intensive workloads, such as those found in research laboratories and high-performance computing (HPC) environments. By selecting the option to import data from and export data to Amazon S3, the solution ensures that data can be easily managed and transferred between the high-performance Lustre file system and the durable, scalable object storage of S3. Mounting the file system on the EC2 instances allows for the distributed processing of the data. Option A, using Amazon FSx for NetApp ONTAP, may not provide the necessary performance characteristics for this use case. Option C, using persistent HDD storage for the Lustre file system, would not meet the required throughput and latency requirements due to the limitations of HDD storage compared to SSD. Option D, with the tiering policy set to NONE, would not ensure that the data is stored on SSD storage, which is critical for achieving the required performance.

解析：To meet the stringent performance requirements of sub-millisecond latencies and a minimum throughput of 6 Gbps, a solutions architect should: B. Create an Amazon S3 bucket to store the raw data and an Amazon FSx for Lustre file system that uses persistent SSD storage. Lustre is a high-performance file system designed for compute-intensive workloads, such as those found in research laboratories and high-performance computing (HPC) environments. By selecting the option to import data from and export data to Amazon S3, the solution ensures that data can be easily managed and transferred between the high-performance Lustre file system and the durable, scalable object storage of S3. Mounting the file system on the EC2 instances allows for the distributed processing of the data. Option A, using Amazon FSx for NetApp ONTAP, may not provide the

necessary performance characteristics for this use case. Option C, using persistent HDD storage for the Lustre file system, would not meet the required throughput and latency requirements due to the limitations of HDD storage compared to SSD. Option D, with the tiering policy set to NONE, would not ensure that the data is stored on SSD storage, which is critical for achieving the required performance.

256. Question #300A 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?

- 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.

答案：C

解析：To migrate the legacy application to AWS Cloud in the most cost-effective manner, considering the application's continuous operation and growing database storage, a solutions architect should: C. Migrate the application layer to Amazon EC2 Reserved Instances and the data storage layer to Amazon Aurora Reserved Instances. Reserved Instances provide significant cost savings over On-Demand pricing for applications that run continuously. Amazon Aurora is a MySQL and PostgreSQL compatible relational database built for the cloud, offering high availability, durability, and automatic scaling. By choosing Reserved Instances for both the application and the database layers, the company can optimize costs while ensuring that the infrastructure meets the performance and storage needs of the application. Option A, using Spot Instances, does not guarantee the necessary capacity for a legacy application that runs

continuously. Option B, using On-Demand Instances for RDS, can be more expensive in the long term due to the lack of reservation discounts. Option D does not specify the use of Aurora, which is optimized for cloud environments and can scale automatically to accommodate growing storage needs.

解析: To migrate the legacy application to AWS Cloud in the most cost-effective manner, considering the application's continuous operation and growing database storage, a solutions architect should: C. Migrate the application layer to Amazon EC2 Reserved Instances and the data storage layer to Amazon Aurora Reserved Instances. Reserved Instances provide significant cost savings over On-Demand pricing for applications that run continuously. Amazon Aurora is a MySQL and PostgreSQL compatible relational database built for the cloud, offering high availability, durability, and automatic scaling. By choosing Reserved Instances for both the application and the database layers, the company can optimize costs while ensuring that the infrastructure meets the performance and storage needs of the application. Option A, using Spot Instances, does not guarantee the necessary capacity for a legacy application that runs continuously. Option B, using On-Demand Instances for RDS, can be more expensive in the long term due to the lack of reservation discounts. Option D does not specify the use of Aurora, which is optimized for cloud environments and can scale automatically to accommodate growing storage needs.

257. Question #301A 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?

- A. AWS Snowcone

- B. AWS DataSync
- C. AWS Transfer Family
- D. AWS Storage Gateway File Gateway

答案：B

解析：To migrate a large amount of data from an on-premises Windows file server to Amazon FSx for Windows File Server while controlling the bandwidth usage and maximizing the performance of the data transfer, the laboratory should use: B. AWS DataSync. DataSync is a data transfer service that automates moving data between on-premises storage and AWS services. It can be used to migrate data to Amazon FSx for Windows File Server, and it allows for bandwidth throttling to control the data transfer rate, minimizing the impact on other departments' network usage. DataSync can also perform the migration within the required 5-day timeframe. Option A, AWS Snowcone, is designed for importing large amounts of data into AWS but is limited to 8 TB per device and may not meet the required speed due to its delivery and setup time. Option C, AWS Transfer Family, provides file transfer protocol (FTP) services but does not offer the same level of bandwidth control or direct migration capabilities to Amazon FSx. Option D, AWS Storage Gateway File Gateway, is used for low-latency access to files stored in S3 but is not designed for the high-performance migration of large datasets within a紧迫的 time frame.

解析：To migrate a large amount of data from an on-premises Windows file server to Amazon FSx for Windows File Server while controlling the bandwidth usage and maximizing the performance of the data transfer, the laboratory should use: B. AWS DataSync. DataSync is a data transfer service that automates moving data between on-premises storage and AWS services. It can be used to migrate data to Amazon FSx for Windows File Server, and it allows for bandwidth throttling to control the data transfer rate, minimizing the impact on other departments' network usage. DataSync can also perform the migration within the required 5-day timeframe. Option A, AWS Snowcone, is designed for importing large amounts of data into AWS but is limited to 8 TB per device and may not meet the required speed due to its delivery and setup time. Option C, AWS

Transfer Family, provides file transfer protocol (FTP) services but does not offer the same level of bandwidth control or direct migration capabilities to Amazon FSx. Option D, AWS Storage Gateway File Gateway, is used for low-latency access to files stored in S3 but is not designed for the high-performance migration of large datasets within a **紧迫的 time frame**.

258. Question #303A 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?

- 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.**

答案: D

解析: To manage the scaling of an Amazon ECS cluster using the Fargate launch type in a cost-effective manner, a solutions architect should: D. Use **AWS Application Auto Scaling with target tracking policies**.

Application Auto Scaling allows you to configure policies that automatically adjust the number of tasks your cluster is running based on the specified target tracking metric. By setting up a target tracking policy, the ECS cluster can scale the number of tasks in response to changes in the tracked metric, such as CPU or memory utilization, ensuring that the application runs efficiently and costs are reduced during periods of lower utilization. Option A is not applicable to Fargate, as Fargate does not require the management of EC2 instances. Option B is not the recommended approach for scaling ECS tasks, as it

involves additional complexity and may not provide the desired scaling behavior. Option C, while it can be used with ECS, does not offer the same level of automation and efficiency as target tracking policies.

解析: To manage the scaling of an Amazon ECS cluster using the Fargate launch type in a cost-effective manner, a solutions architect should: D. Use AWS Application Auto Scaling with target tracking policies.

Application Auto Scaling allows you to configure policies that automatically adjust the number of tasks your cluster is running based on the specified target tracking metric. By setting up a target tracking policy, the ECS cluster can scale the number of tasks in response to changes in the tracked metric, such as CPU or memory utilization, ensuring that the application runs efficiently and costs are reduced during periods of lower utilization. Option A is not applicable to Fargate, as Fargate does not require the management of EC2 instances. Option B is not the recommended approach for scaling ECS tasks, as it involves additional complexity and may not provide the desired scaling behavior. Option C, while it can be used with ECS, does not offer the same level of automation and efficiency as target tracking policies.

259. Question #304A 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?

- 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).

答案: A

解析: To transfer large amounts of data between NFS file systems in different AWS Regions with minimal operational overhead, a solutions architect should: A. Use AWS DataSync. DataSync is a managed service that can automatically transfer files between on-premises storage and AWS services, including between different AWS Regions. It is designed to

handle large-scale data transfers and can be scheduled to operate periodically, making it a low-overhead solution for recurring data transfers. Option B, AWS Snowball devices, are more suitable for one-time or less frequent data transfers due to the physical transportation process involved. Option C, setting up an SFTP server on Amazon EC2, would require more management and configuration to achieve the same level of automation and reliability as DataSync. Option D, AWS DMS, is primarily used for database migration and replication, not for general file system data transfers.

解析: To transfer large amounts of data between NFS file systems in different AWS Regions with minimal operational overhead, a solutions architect should: A. Use AWS DataSync. DataSync is a managed service that can automatically transfer files between on-premises storage and AWS services, including between different AWS Regions. It is designed to handle large-scale data transfers and can be scheduled to operate periodically, making it a low-overhead solution for recurring data transfers. Option B, AWS Snowball devices, are more suitable for one-time or less frequent data transfers due to the physical transportation process involved. Option C, setting up an SFTP server on Amazon EC2, would require more management and configuration to achieve the same level of automation and reliability as DataSync. Option D, AWS DMS, is primarily used for database migration and replication, not for general file system data transfers.

260. Question #305A 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?

- 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.

答案: C

解析: To create a fully managed shared storage solution that supports SMB client access for a gaming application, a solutions architect should: C. Create an Amazon FSx for Windows File Server file system. FSx for Windows File Server is a fully managed service that provides a scalable, high-performance file system that is accessible via the SMB protocol. It is designed to seamlessly integrate with the AWS environment, making it an ideal choice for applications that require shared access to data. Option A, AWS DataSync, is used for transferring data between storage locations and not for providing a shared file system. Option B, setting up an EC2 Windows instance, would require management of the file share and is not a fully managed solution. Option D, using Amazon S3 with an IAM role, does not provide native SMB access and would require additional configuration and management.

解析: To create a fully managed shared storage solution that supports SMB client access for a gaming application, a solutions architect should: C. Create an Amazon FSx for Windows File Server file system. FSx for Windows File Server is a fully managed service that provides a scalable, high-performance file system that is accessible via the SMB protocol. It is designed to seamlessly integrate with the AWS environment, making it an ideal choice for applications that require shared access to data. Option A, AWS DataSync, is used for transferring data between storage locations and not for providing a shared file system. Option B, setting up an EC2 Windows instance, would require management of the file share and is not a fully managed solution. Option D, using Amazon S3 with an IAM role, does not provide native SMB access and would require additional configuration and management.

261. Question #306A company wants to run an in-memory database for a **latency-sensitive** application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and **requires high network throughput**. A solutions architect needs to provide a **cost-effective** network design that minimizes data transfer charges. Which solution meets these requirements?

- A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
- B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
- C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
- D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

答案：A

解析：For a latency-sensitive application that requires high network throughput and processes a large number of transactions, a solutions architect should: A. Launch all EC2 instances in the same Availability Zone within the same AWS Region and use a placement group with a cluster strategy. **This approach ensures that the instances are physically close to each other, which reduces network latency and increases network throughput between instances.** The cluster placement group is designed to optimize performance for applications that require a high level of network connectivity and low latency. Option B, launching instances in different Availability Zones, would increase network latency due to the distance between zones. Option C and D, deploying an Auto Scaling group, do not directly address the need for low latency and high network throughput, and they may also result in higher data transfer charges due to inter-AZ communication.

解析：For a latency-sensitive application that requires high network throughput and processes a large number of transactions, a solutions architect should: A. Launch all EC2 instances in the same Availability

Zone within the same AWS Region and use a placement group with a cluster strategy. This approach ensures that the instances are physically close to each other, which reduces network latency and increases network throughput between instances. The cluster placement group is designed to optimize performance for applications that require a high level of network connectivity and low latency. Option B, launching instances in different Availability Zones, would increase network latency due to the distance between zones. Option C and D, deploying an Auto Scaling group, do not directly address the need for low latency and high network throughput, and they may also result in higher data transfer charges due to inter-AZ communication.

262. Question #307A 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?

- 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

答案: D

解析: To migrate to AWS while minimizing the need to scale on-premises iSCSI storage and keeping only recently accessed data locally, the company should use: D. AWS Storage Gateway Volume Gateway cached volumes. This solution allows the company to store frequently accessed data on-premises while asynchronously backing up the entire dataset to AWS, which is stored in Amazon S3. The cached volume configuration is designed to provide low-latency access to the most commonly used data, while less frequently accessed data is stored in the cloud, reducing the need for on-premises storage scaling. Option A, Amazon S3 File Gateway, is designed for file-level transfers and does not provide block-level storage required for iSCSI. Option B, Tape Gateway, is used for backup

and archive purposes rather than primary storage. Option C, stored volumes, would store the entire dataset on-premises, which does not align with the goal of minimizing on-premises storage.

解析: To migrate to AWS while minimizing the need to scale on-premises iSCSI storage and keeping only recently accessed data locally, the company should use: D. AWS Storage Gateway Volume Gateway cached volumes. This solution allows the company to store frequently accessed data on-premises while asynchronously backing up the entire dataset to AWS, which is stored in Amazon S3. The cached volume configuration is designed to provide low-latency access to the most commonly used data, while less frequently accessed data is stored in the cloud, reducing the need for on-premises storage scaling. Option A, Amazon S3 File Gateway, is designed for file-level transfers and does not provide block-level storage required for iSCSI. Option B, Tape Gateway, is used for backup and archive purposes rather than primary storage. Option C, stored volumes, would store the entire dataset on-premises, which does not align with the goal of minimizing on-premises storage.

263. Question #309A 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**?

- 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.

答案: A

解析: To optimize storage costs by identifying underutilized S3 buckets with minimal operational overhead, a solutions architect should: A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics. S3 Storage Lens provides detailed metrics and insights into the usage patterns of S3 buckets, which can help identify buckets that are infrequently accessed or no longer needed. This information can be used to optimize storage costs by deleting or archiving data in those buckets. Option B, using the S3 dashboard in the AWS Management Console, provides limited visibility into bucket usage and does not offer advanced activity metrics. Option C, using Amazon CloudWatch and Amazon Athena, would require additional setup and management of metrics and queries, which increases operational overhead. Option D, using AWS CloudTrail and CloudWatch Logs, is more focused on security and access auditing rather than analyzing access patterns for cost optimization.

解析: To optimize storage costs by identifying underutilized S3 buckets with minimal operational overhead, a solutions architect should: A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics. S3 Storage Lens provides detailed metrics and insights into the usage patterns of S3 buckets, which can help identify buckets that are infrequently accessed or no longer needed. This information can be used to optimize storage costs by deleting or archiving data in those buckets. Option B, using the S3 dashboard in the AWS Management Console, provides limited visibility into bucket usage and does not offer advanced activity metrics. Option C, using Amazon CloudWatch and Amazon Athena, would require additional setup and management of metrics and queries, which increases operational overhead. Option D, using AWS CloudTrail and CloudWatch Logs, is more focused on security and access auditing rather than analyzing access patterns for cost optimization.

264. Question #310A 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 associated with data transfers and wants to maintain or improve performance. What should a solutions architect do to meet these requirements?

- 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.

答案：B

解析：To reduce data transfer costs and maintain or improve performance for customers distributed across North America and Europe, a solutions architect should: B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL and switch to CloudFront signed URLs for access control. CloudFront is a global content delivery network (CDN) that caches content at edge locations closer to customers, reducing latency and improving the download experience. By using CloudFront, the company can also reduce data transfer costs associated with serving content from the origin S3 bucket, especially for customers outside the us-east-1 Region. Option A, S3 Transfer Acceleration, is designed to speed up the uploading of files to S3 and is not optimized for the distribution of large files to end users. Option C, setting up a second S3 bucket with Cross-Region

Replication, would incur additional costs for replication and may not be as performant as using a CDN. Option D, modifying the web application for streaming, would require managing the complexity of streaming data directly and is not as efficient as leveraging a CDN for content delivery.

解析: To reduce data transfer costs and maintain or improve performance for customers distributed across North America and Europe, a solutions architect should: B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL and switch to CloudFront signed URLs for access control. CloudFront is a global content delivery network (CDN) that caches content at edge locations closer to customers, reducing latency and improving the download experience. By using CloudFront, the company can also reduce data transfer costs associated with serving content from the origin S3 bucket, especially for customers outside the us-east-1 Region. Option A, S3 Transfer Acceleration, is designed to speed up the uploading of files to S3 and is not optimized for the distribution of large files to end users. Option C, setting up a second S3 bucket with Cross-Region Replication, would incur additional costs for replication and may not be as performant as using a CDN. Option D, modifying the web application for streaming, would require managing the complexity of streaming data directly and is not as efficient as leveraging a CDN for content delivery.

265. Question #311A 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?

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.

答案：C

解析：To design a web application that efficiently processes insurance quotes while ensuring quotes are separated by type, responded to within 24 hours, and not lost, a solutions architect should: C. Create a single Amazon SNS topic and subscribe multiple Amazon SQS queues to it. Use SNS message filtering to direct messages to the appropriate SQS queue based on quote type. Each backend application server can then process messages from its own SQS queue. This setup ensures that quotes are separated by type, can be processed within the required time frame, and are not lost. SQS guarantees message delivery and provides a scalable and durable message queuing system. Using SNS for message publishing and SQS for message processing maximizes operational efficiency and minimizes maintenance. Option A, using Amazon Kinesis, is more suitable for real-time processing of streaming data rather than queuing messages for asynchronous processing. Option B, using AWS Lambda with Amazon SNS, does not provide the same level of guaranteed message delivery and separation by quote type as SQS. Option D, using Amazon Kinesis Data Firehose with Amazon OpenSearch Service, is not as efficient for queuing and processing individual quote requests as using SNS and SQS.

解析: To design a web application that efficiently processes insurance quotes while ensuring quotes are separated by type, responded to within 24 hours, and not lost, a solutions architect should: C. Create a single Amazon SNS topic and subscribe multiple Amazon SQS queues to it. Use SNS message filtering to direct messages to the appropriate SQS queue based on quote type. Each backend application server can then process messages from its own SQS queue. This setup ensures that quotes are separated by type, can be processed within the required time frame, and are not lost. SQS guarantees message delivery and provides a scalable and durable message queuing system. Using SNS for message publishing and SQS for message processing maximizes operational efficiency and minimizes maintenance. Option A, using Amazon Kinesis, is more suitable for real-time processing of streaming data rather than queuing messages for asynchronous processing. Option B, using AWS Lambda with Amazon SNS, does not provide the same level of guaranteed message delivery and separation by quote type as SQS. Option D, using Amazon Kinesis Data Firehose with Amazon OpenSearch Service, is not as efficient for queuing and processing individual quote requests as using SNS and SQS.

266. Question #312A 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?

- 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.

答案：B

解析：For an operationally efficient way to back up an application running on Amazon EC2 instances with attached EBS volumes and ensure recoverability in a different AWS Region, a solutions architect should:
B. Create a backup plan using AWS Backup, which is designed to automate and manage backups across AWS services. By adding the application's EC2 instances as resources, the entire configuration and data of the instances, including the EBS volumes, can be backed up nightly. AWS Backup also allows for copying backups to another Region, providing disaster recovery capabilities. Option A, writing a custom AWS Lambda function, would require additional development and maintenance effort. Option C, while it does include EBS volumes in the backup, does not explicitly mention backing up the EC2 instance configurations. Option D, copying snapshots to a different Availability Zone, does not provide the cross-Region recovery that is required.

解析：For an operationally efficient way to back up an application running on Amazon EC2 instances with attached EBS volumes and ensure recoverability in a different AWS Region, a solutions architect should:
B. Create a backup plan using AWS Backup, which is designed to automate and manage backups across AWS services. By adding the application's EC2 instances as resources, the entire configuration and data of the instances, including the EBS volumes, can be backed up nightly. AWS Backup also allows for copying backups to another Region, providing disaster recovery capabilities. Option A, writing a custom AWS Lambda function, would require additional development and maintenance effort. Option C, while it does include EBS volumes in the backup, does not explicitly mention backing up the EC2 instance configurations. Option D, copying snapshots to a different Availability Zone, does not provide the cross-Region recovery that is required.

267. Question #313A 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?

- 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.

答案: C

解析: To build a platform that allows authorized users to access the company's content on their mobile devices, a solutions architect should:

C. Use Amazon CloudFront, which is a content delivery network (CDN) service that can securely deliver content to users worldwide with low latency and high transfer speeds. By providing signed URLs, the company can control access to its content, ensuring that only authorized users can view the content on their mobile devices. Option A, publishing content to a public Amazon S3 bucket, does not provide a mechanism for controlling access to the content. Option B, setting up an IPsec VPN, is not practical for millions of users and is typically used for site-to-site connections. Option D, setting up AWS Client VPN, is more suitable for providing secure access to internal resources rather than streaming content to a large number of mobile users.

解析: To build a platform that allows authorized users to access the company's content on their mobile devices, a solutions architect should:

C. Use Amazon CloudFront, which is a content delivery network (CDN) service that can securely deliver content to users worldwide with low latency and high transfer speeds. By providing signed URLs, the company can control access to its content, ensuring that only authorized users can view the content on their mobile devices. Option A, publishing content to a public Amazon S3 bucket, does not provide a mechanism for

controlling access to the content. Option B, setting up an IPsec VPN, is not practical for millions of users and is typically used for site-to-site connections. Option D, setting up AWS Client VPN, is more suitable for providing secure access to internal resources rather than streaming content to a large number of mobile users.

268. Question #314A 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?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL**
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

答案：B

解析：Given the requirement for minimal downtime and the need to accommodate future growth in users without specifying an instance type, a solutions architect should recommend: B. Amazon Aurora Serverless for MySQL. This service is a fully managed, serverless database option that automatically scales up or down based on the application's needs. It provides high availability and is designed to have minimal downtime, which is suitable for the sales team's requirements. Additionally, because it does not require the selection of a specific instance type, it allows for flexibility in handling an increase in users. Option A, Amazon Aurora MySQL, would require the selection of an instance type, which does not align with the database administrator's preference. Option C, Amazon Redshift Spectrum, is designed for large-scale data warehousing and is not suitable for direct migration of an on-premises MySQL database. Option D, Amazon RDS for MySQL, also requires the selection of an instance type and does not offer the serverless, automatic scaling capabilities that Aurora Serverless provides.

解析: Given the requirement for minimal downtime and the need to accommodate future growth in users without specifying an instance type, a solutions architect should recommend: B. Amazon Aurora Serverless for MySQL. This service is a fully managed, serverless database option that automatically scales up or down based on the application's needs. It provides high availability and is designed to have minimal downtime, which is suitable for the sales team's requirements. Additionally, because it does not require the selection of a specific instance type, it allows for flexibility in handling an increase in users. Option A, Amazon Aurora MySQL, would require the selection of an instance type, which does not align with the database administrator's preference. Option C, Amazon Redshift Spectrum, is designed for large-scale data warehousing and is not suitable for direct migration of an on-premises MySQL database. Option D, Amazon RDS for MySQL, also requires the selection of an instance type and does not offer the serverless, automatic scaling capabilities that Aurora Serverless provides.

269. Question #315A 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?

- 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.

答案：D

解析：To actively scan for vulnerabilities on EC2 instances and generate detailed reports of the findings, a solutions architect should: D. Turn on Amazon Inspector and deploy the Inspector agent to the EC2 instances.

Amazon Inspector is a security assessment service that automates the identification of vulnerabilities and security issues in applications running on EC2 instances. By deploying the Inspector agent, the company can perform security assessments and receive detailed reports.

Additionally, configuring an AWS Lambda function to automate the generation and distribution of these reports ensures that the findings are communicated effectively. Option A, AWS Shield, primarily provides DDoS protection and does not scan for vulnerabilities. Option B, Amazon Macie, is designed to discover and protect sensitive data, not to perform vulnerability assessments. Option C, Amazon GuardDuty, is a threat detection service that monitors AWS accounts and resources for malicious activity, but it does not deploy agents to EC2 instances for vulnerability scanning.

解析：To actively scan for vulnerabilities on EC2 instances and generate detailed reports of the findings, a solutions architect should: D. Turn on Amazon Inspector and deploy the Inspector agent to the EC2 instances.

Amazon Inspector is a security assessment service that automates the identification of vulnerabilities and security issues in applications running on EC2 instances. By deploying the Inspector agent, the company can perform security assessments and receive detailed reports.

Additionally, configuring an AWS Lambda function to automate the generation and distribution of these reports ensures that the findings are communicated effectively. Option A, AWS Shield, primarily provides DDoS protection and does not scan for vulnerabilities. Option B, Amazon Macie, is designed to discover and protect sensitive data, not to perform vulnerability assessments. Option C, Amazon GuardDuty, is a threat detection service that monitors AWS accounts and resources for malicious activity, but it does not deploy agents to EC2 instances for vulnerability scanning.

270. Question #316A 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?

- 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.

答案: C

解析: To reduce operational costs and maintain the ability to process an increasing number of messages in an SQS queue, a solutions architect should: C. Migrate the script on the EC2 instance to an AWS Lambda function. AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. By migrating the script to a Lambda function, the company can take advantage of Lambda's automatic scaling and pay-per-use pricing model, which can significantly reduce operational costs compared to maintaining a constant EC2 instance. Option A, increasing the size of the EC2 instance, would increase costs without providing a scalable solution. Option B, using Amazon EventBridge, does not directly address the need to process messages from an SQS queue. Option D, using AWS Systems Manager Run Command, would still require an EC2 instance to be running and would not offer the scalability or cost benefits of a serverless solution like Lambda.

解析: To reduce operational costs and maintain the ability to process an increasing number of messages in an SQS queue, a solutions architect should: C. Migrate the script on the EC2 instance to an AWS Lambda function. AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. By migrating the script to a Lambda function, the company can take advantage of Lambda's automatic scaling and pay-per-use pricing model, which can significantly

reduce operational costs compared to maintaining a constant EC2 instance. Option A, increasing the size of the EC2 instance, would increase costs without providing a scalable solution. Option B, using Amazon EventBridge, does not directly address the need to process messages from an SQS queue. Option D, using AWS Systems Manager Run Command, would still require an EC2 instance to be running and would not offer the scalability or cost benefits of a serverless solution like Lambda.

271. Question #317A 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?

- 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.

答案：A

解析: To enable the COTS application to use data produced by the legacy application with minimal operational overhead, a solutions architect should: A. Create an AWS Glue ETL job that runs on a schedule. AWS Glue is a fully managed ETL service that can automate the process of transforming data from its source in S3 into the desired format for analysis in Redshift. By configuring the ETL job to convert .csv files to a format compatible with Redshift, the company can use the COTS application to perform SQL queries on the transformed data. Option B, developing a Python script to run on EC2 instances, would require managing servers and may not be as scalable or cost-effective. Option C, using AWS Lambda and DynamoDB, would not be suitable for large-scale data processing and storage needs. Option D, using Amazon EventBridge and EMR, would involve more operational complexity and overhead compared to the managed service provided by AWS Glue.

解析: To enable the COTS application to use data produced by the legacy application with minimal operational overhead, a solutions architect should: A. Create an AWS Glue ETL job that runs on a schedule. AWS Glue is a fully managed ETL service that can automate the process of transforming data from its source in S3 into the desired format for analysis in Redshift. By configuring the ETL job to convert .csv files to a format compatible with Redshift, the company can use the COTS application to perform SQL queries on the transformed data. Option B, developing a Python script to run on EC2 instances, would require managing servers and may not be as scalable or cost-effective. Option C, using AWS Lambda and DynamoDB, would not be suitable for large-scale data processing and storage needs. Option D, using Amazon EventBridge and EMR, would involve more operational complexity and overhead compared to the managed service provided by AWS Glue.

272. Question #319A 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?**

- 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.

答案：A

解析：To provide secure access to EC2 instances without the need for managing SSH keys, a solutions architect should: A. Use AWS Systems Manager Session Manager to connect to the EC2 instances. **Session Manager is a fully managed service that provides secure and auditable instance management without the need for SSH keys. It works through the AWS Management Console and does not require any additional infrastructure or software on the EC2 instances.** This approach reduces administrative overhead by eliminating the need to manage and distribute SSH keys. Option B, using AWS STS to generate one-time SSH keys, would require additional setup and management of the keys. Option C, setting up bastion instances, involves managing an additional layer of infrastructure. Option D, using Amazon Cognito and AWS Lambda, would require the development and maintenance of custom authentication mechanisms, which adds complexity and overhead. The provided answers and explanations are based on the information given in the questions and the context of AWS services. The solutions recommended aim to address the specific requirements stated in each scenario while considering factors like cost, security, manageability, and AWS best practices.

解析：To provide secure access to EC2 instances without the need for managing SSH keys, a solutions architect should: A. Use AWS Systems Manager Session Manager to connect to the EC2 instances. **Session Manager is a fully managed service that provides secure and auditable instance management without the need for SSH keys. It works through the AWS Management Console and does not require any additional infrastructure or software on the EC2 instances.**

Management Console and does not require any additional infrastructure or software on the EC2 instances. This approach reduces administrative overhead by eliminating the need to manage and distribute SSH keys. Option B, using AWS STS to generate one-time SSH keys, would require additional setup and management of the keys. Option C, setting up bastion instances, involves managing an additional layer of infrastructure. Option D, using Amazon Cognito and AWS Lambda, would require the development and maintenance of custom authentication mechanisms, which adds complexity and overhead. The provided answers and explanations are based on the information given in the questions and the context of AWS services. The solutions recommended aim to address the specific requirements stated in each scenario while considering factors like cost, security, manageability, and AWS best practices.

273. Question #320A 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?**

- 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.

答案: A

解析: The solution that meets the requirements for near-real-time data querying, scalability, and minimal data loss is to publish data to Amazon Kinesis Data Streams. This service can handle ingestion rates up to 1

MB/s and provides real-time data processing. Kinesis Data Analytics can be used to query the data with low latency. Additionally, Kinesis Data Streams has a default persistent data store that retains data for up to 7 days, which ensures minimal data loss in the event of an EC2 instance reboot.

解析：The solution that meets the requirements for near-real-time data querying, scalability, and minimal data loss is to publish data to Amazon Kinesis Data Streams. This service can handle ingestion rates up to 1 MB/s and provides real-time data processing. Kinesis Data Analytics can be used to query the data with low latency. Additionally, Kinesis Data Streams has a default persistent data store that retains data for up to 7 days, which ensures minimal data loss in the event of an EC2 instance reboot.

274. Question #321 What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are **encrypted**?

- 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.

答案：D

解析：To ensure all objects uploaded to an Amazon S3 bucket are encrypted, the solutions architect should update the bucket policy to deny any PutObject requests that do not have the x-amz-server-side-encryption header set. This enforces the use of server-side encryption for all objects, ensuring that they are encrypted upon upload.

解析：To ensure all objects uploaded to an Amazon S3 bucket are encrypted, the solutions architect should update the bucket policy to deny any PutObject requests that do not have the

x-amz-server-side-encryption header set. This enforces the use of server-side encryption for all objects, ensuring that they are encrypted upon upload.

275. Question #322A 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?

- 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.

答案: C

解析: To provide a faster response time to users and handle the asynchronous nature of thumbnail generation, the solutions architect should create an Amazon SQS message queue. This allows the image upload process to place a message on the queue for thumbnail generation without

waiting for the process to complete. The user can be alerted immediately that the image was received, while the thumbnail generation proceeds in the background.

解析: To provide a faster response time to users and handle the asynchronous nature of thumbnail generation, the solutions architect should create an Amazon SQS message queue. This allows the image upload process to place a message on the queue for thumbnail generation without waiting for the process to complete. The user can be alerted immediately that the image was received, while the thumbnail generation proceeds in the background.

276. Question #323A 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?

- 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.

答案: B

解析: To ensure a highly available system that can process messages from badge readers and make the results available for analysis, the solutions

architect should recommend creating an HTTPS endpoint in Amazon API Gateway. This endpoint can be configured to invoke an AWS Lambda function, which will process the incoming messages. The results can then be saved to an Amazon DynamoDB table, which is a scalable and highly available NoSQL database service. This setup allows for the serverless processing of messages and provides a reliable storage solution for the security team's analysis.

解析: To ensure a highly available system that can process messages from badge readers and make the results available for analysis, the solutions architect should recommend creating an HTTPS endpoint in Amazon API Gateway. This endpoint can be configured to invoke an AWS Lambda function, which will process the incoming messages. The results can then be saved to an Amazon DynamoDB table, which is a scalable and highly available NoSQL database service. This setup allows for the serverless processing of messages and provides a reliable storage solution for the security team's analysis.

277. Question #324A 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?

- 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.

答案: D

解析: To meet the requirement of least amount of change to the existing infrastructure while ensuring high availability and immediate access to all file types, the solutions architect should recommend provisioning an AWS Storage Gateway Volume Gateway stored volume. This solution allows the existing file server to connect to the stored volume via iSCSI, just as it does with the current on-premises storage, and copy all files to the new storage volume. Scheduled snapshots can be configured to ensure data protection, and in the event of a disaster, a snapshot can be restored to an Amazon EBS volume and attached to an EC2 instance for recovery. This approach requires minimal changes to the current setup and maintains low latency access.

解析: To meet the requirement of least amount of change to the existing infrastructure while ensuring high availability and immediate access to all file types, the solutions architect should recommend provisioning an AWS Storage Gateway Volume Gateway stored volume. This solution allows the existing file server to connect to the stored volume via iSCSI, just as it does with the current on-premises storage, and copy all files to the new storage volume. Scheduled snapshots can be configured to ensure

data protection, and in the event of a disaster, a snapshot can be restored to an Amazon EBS volume and attached to an EC2 instance for recovery. This approach requires minimal changes to the current setup and maintains low latency access.

278. Question #325A 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?

- 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.

答案：A

解析：To resolve the issue of users being unable to access protected content, the solutions architect should update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content. This ensures that the authenticated users receive the necessary permissions to access the resources stored in the S3 bucket through the JWT token provided by Cognito. This approach directly addresses the permission issue and is aligned with AWS best practices for granting access to resources based on identity authentication.

解析：To resolve the issue of users being unable to access protected content, the solutions architect should update the Amazon Cognito

identity pool to assume the proper IAM role for access to the protected content. This ensures that the authenticated users receive the necessary permissions to access the resources stored in the S3 bucket through the JWT token provided by Cognito. This approach directly addresses the permission issue and is aligned with AWS best practices for granting access to resources based on identity authentication.

279. Question #327A 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?

- 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.

答案: A

解析: To meet the requirement of allowing access only to approved third-party software repositories while blocking other internet traffic, the solutions architect should update the route table for the private subnet to route outbound traffic to an AWS Network Firewall. **This firewall can be configured with domain list rule groups that specifically allow traffic to the required URLs while blocking all other traffic.** This approach provides a secure and compliant method to control the EC2 instances' outbound access to the internet.

解析: To meet the requirement of allowing access only to approved third-party software repositories while blocking other internet traffic, the solutions architect should update the route table for the private subnet to route outbound traffic to an AWS Network Firewall. This firewall can be configured with domain list rule groups that specifically allow traffic to the required URLs while blocking all other traffic. This approach provides a secure and compliant method to control the EC2 instances' outbound access to the internet.

280. Question #328A 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?

- 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.

答案: D

解析: To ensure that all requests are processed successfully during a significant increase in sales requests, the solutions architect should recommend adding an Amazon CloudFront distribution for the static content

to offload and cache the static assets closer to the users. Additionally, adding an Amazon SQS queue will help decouple the request handling from the EC2 instances, allowing for asynchronous processing of the sales requests. This ensures that even if there is a sudden spike in traffic, the requests can be queued and processed successfully without user perception of failure.

解析: To ensure that all requests are processed successfully during a significant increase in sales requests, the solutions architect should recommend adding an Amazon CloudFront distribution for the static content to offload and cache the static assets closer to the users. Additionally, adding an Amazon SQS queue will help decouple the request handling from the EC2 instances, allowing for asynchronous processing of the sales requests. This ensures that even if there is a sudden spike in traffic, the requests can be queued and processed successfully without user perception of failure.

281. Question #329A 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?

- 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.

答案: D

解析: To automate the process of scanning for vulnerabilities and patching EC2 instances, the solutions architect should use Amazon Inspector to scan the instances for software vulnerabilities. Amazon Inspector is a security assessment service that identifies potential security issues. By configuring Amazon Inspector, the architect can schedule regular scans. Additionally, AWS Systems Manager Patch Manager can be set up to apply patches to the EC2 instances on a regular schedule, and it can provide patch status reports, fulfilling the requirement for regular security maintenance.

解析: To automate the process of scanning for vulnerabilities and patching EC2 instances, the solutions architect should use Amazon Inspector to scan the instances for software vulnerabilities. Amazon Inspector is a security assessment service that identifies potential security issues. By configuring Amazon Inspector, the architect can schedule regular scans. Additionally, AWS Systems Manager Patch Manager can be set up to apply patches to the EC2 instances on a regular schedule, and it can provide patch status reports, fulfilling the requirement for regular security maintenance.

282. Question #330A 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?

- 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.

答案: A

解析: To meet the requirement for encrypting data at rest on Amazon RDS DB instances, the solutions architect should create a key in AWS Key

Management Service (AWS KMS) and enable encryption for the DB instances.

AWS KMS is designed to manage cryptographic keys used to encrypt data, and integrating it with RDS ensures that the data is encrypted at rest.

This approach is the most straightforward and secure method for achieving the company's encryption requirements.

解析：To meet the requirement for encrypting data at rest on Amazon RDS DB instances, the solutions architect should create a key in AWS Key Management Service (AWS KMS) and enable encryption for the DB instances. AWS KMS is designed to manage cryptographic keys used to encrypt data, and integrating it with RDS ensures that the data is encrypted at rest. This approach is the most straightforward and secure method for achieving the company's encryption requirements.

283. Question #331A 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?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

答案：A

解析：Given the limited bandwidth and the large amount of data that needs to be migrated within a tight deadline, the solutions architect should use AWS Snowball. AWS Snowball is a petabyte-scale data migration service that can transfer large amounts of data into and out of AWS. It is particularly well-suited for situations where high-bandwidth is not available, as it involves shipping a storage device to the customer's location, copying the data to the device, and then shipping it back to AWS for uploading to the cloud.

解析：Given the limited bandwidth and the large amount of data that needs to be migrated within a tight deadline, the solutions architect should use AWS Snowball. AWS Snowball is a petabyte-scale data migration service that can transfer large amounts of data into and out of AWS. It is

particularly well-suited for situations where high-bandwidth is not available, as it involves shipping a storage device to the customer's location, copying the data to the device, and then shipping it back to AWS for uploading to the cloud.

284. Question #332A 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?

- 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).

答案：B

解析：To securely provide access to confidential and sensitive files while ensuring that only authorized users can access them, the solutions architect should migrate the files to an Amazon FSx for Windows File Server file system. This service is designed to provide a scalable, high-performance file system that can be integrated with an existing on-premises Active Directory, allowing for the use of existing permissions and user accounts. By configuring AWS Client VPN, the company can establish a secure VPN connection for employees to access the file system, addressing both the security and capacity requirements.

解析: To securely provide access to confidential and sensitive files while ensuring that only authorized users can access them, the solutions architect should migrate the files to an Amazon FSx for Windows File Server file system. This service is designed to provide a scalable, high-performance file system that can be integrated with an existing on-premises Active Directory, allowing for the use of existing permissions and user accounts. By configuring AWS Client VPN, the company can establish a secure VPN connection for employees to access the file system, addressing both the security and capacity requirements.

285. Question #333A 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?

- 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.

答案: C

解析: To handle the predictable workload spike that occurs on the first day of every month, the solutions architect should recommend configuring an EC2 Auto Scaling scheduled scaling policy. This allows for the proactive scaling of EC2 instances in anticipation of the increased load. By scheduling the scaling event to increase the number of instances before the batch run begins, the application can handle the workload effectively and maintain performance, thus avoiding downtime.

解析: To handle the predictable workload spike that occurs on the first day of every month, the solutions architect should recommend configuring an EC2 Auto Scaling scheduled scaling policy. This allows for the proactive scaling of EC2 instances in anticipation of the increased load. By scheduling the scaling event to increase the number of instances before the batch run begins, the application can handle the workload effectively and maintain performance, thus avoiding downtime.

286. Question #334A 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?**

- 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).

答案: A

解析: To enable the customer to use their on-premises Microsoft Active Directory for accessing files in Amazon S3 without changing the customer's application, the solutions architect should set up AWS Transfer Family with SFTP for Amazon S3. This service **supports integration with Active Directory for authentication, allowing the customer to use their existing credentials and authorization mechanisms.** This approach has the least operational overhead as it leverages the customer's existing infrastructure and does not require changes to the application or the creation of additional AWS resources.

解析: To enable the customer to use their on-premises Microsoft Active Directory for accessing files in Amazon S3 without changing the customer's application, the solutions architect should set up AWS Transfer Family with SFTP for Amazon S3. This service supports integration with Active Directory for authentication, allowing the customer to use their existing credentials and authorization mechanisms. This approach has the least operational overhead as it leverages the customer's existing infrastructure and does not require changes to the application or the creation of additional AWS resources.

287. Question #335A 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?

- 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.

答案: B

解析: To minimize initialization latency when provisioning large Amazon EC2 instances to meet sudden increases in demand, the solutions architect should enable Amazon EBS fast snapshot restore on a snapshot and provision an AMI from that snapshot. This feature allows for rapid restoration of EBS volumes from snapshots, which in turn reduces the time required to initialize instances from the AMI. Once the new AMI is

available, it can replace the existing AMI in the Auto Scaling group, ensuring that new instances are launched with the updated image and are ready to handle the increased demand quickly.

解析: To minimize initialization latency when provisioning large Amazon EC2 instances to meet sudden increases in demand, the solutions architect should enable Amazon EBS fast snapshot restore on a snapshot and provision an AMI from that snapshot. This feature allows for rapid restoration of EBS volumes from snapshots, which in turn reduces the time required to initialize instances from the AMI. Once the new AMI is available, it can replace the existing AMI in the Auto Scaling group, ensuring that new instances are launched with the updated image and are ready to handle the increased demand quickly.

288. Question #336A 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**?

- 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.

答案：A

解析：To meet the IT security guidelines with the least operational effort, the solutions architect should create a new AWS KMS encryption key and use AWS Secrets Manager to create a new secret. This secret will use the KMS key for encrypting the database credentials. The secret can then be associated with the Aurora DB cluster, and a custom rotation period of 14 days can be configured. AWS Secrets Manager automates the process of rotating the credentials, which reduces the operational effort required to maintain compliance with the security guidelines.

解析：To meet the IT security guidelines with the least operational effort, the solutions architect should create a new AWS KMS encryption key and use AWS Secrets Manager to create a new secret. This secret will use the KMS key for encrypting the database credentials. The secret can then be associated with the Aurora DB cluster, and a custom rotation period of 14 days can be configured. AWS Secrets Manager automates the process of rotating the credentials, which reduces the operational effort required to maintain compliance with the security guidelines.

289. Question #337A 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?

- 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.

答案：A

解析：To reduce replication lag and minimize changes to the application code and operational overhead, the solutions architect should migrate the database to Amazon Aurora MySQL. Aurora provides better performance and scalability compared to standard Amazon RDS for MySQL. By replacing the read replicas with Aurora Replicas and configuring Aurora Auto Scaling, the database can handle increased traffic more effectively, reducing lag. Aurora MySQL also supports native functions that can replace stored procedures, which can help to optimize performance without significant changes to the application code.

解析：To reduce replication lag and minimize changes to the application code and operational overhead, the solutions architect should migrate the database to Amazon Aurora MySQL. Aurora provides better performance and scalability compared to standard Amazon RDS for MySQL. By replacing the read replicas with Aurora Replicas and configuring Aurora Auto Scaling, the database can handle increased traffic more effectively, reducing lag. Aurora MySQL also supports native functions that can replace stored procedures, which can help to optimize performance without significant

changes to the application code.

290. Question #338A 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**?

- 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.

答案: D

解析: The most cost-effective solution for creating a disaster recovery plan that replicates data to a secondary AWS Region is to set up an Aurora global database for the DB cluster. By specifying a minimum of one DB instance in the secondary Region, the company ensures that data is replicated and remains available in the event of a disaster in the primary Region. Aurora global databases provide a fully managed and highly available solution that automatically handles the replication and failover process, which is both cost-effective and minimizes operational overhead.

解析: The most cost-effective solution for creating a disaster recovery plan that replicates data to a secondary AWS Region is to set up an Aurora global database for the DB cluster. By specifying a minimum of one DB instance in the secondary Region, the company ensures that data is replicated and remains available in the event of a disaster in the primary Region. Aurora global databases provide a fully managed and highly available solution that automatically handles the replication and

failover process, which is both cost-effective and minimizes operational overhead.

291. Question #339A 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?

- 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.

答案: C

解析: To secure the custom application with the least amount of programming effort, the solutions architect should store the database credentials in AWS Secrets Manager and configure the application to load these credentials. Secrets Manager provides a secure way to store, manage, and retrieve database credentials. Additionally, setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager automates the rotation process, enhancing security without requiring significant programming effort.

解析: To secure the custom application with the least amount of programming effort, the solutions architect should store the database credentials in AWS Secrets Manager and configure the application to load these credentials. Secrets Manager provides a secure way to store, manage, and retrieve database credentials. Additionally, setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager automates the rotation process, enhancing security without requiring significant programming effort.

292. Question #340A 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?

- 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.

答案: A

解析: To resolve the SQL injection vulnerability, the company should use AWS WAF (Web Application Firewall) in front of the Application Load Balancer (ALB). **AWS WAF can be configured with web ACLs that include rules to detect and block SQL injection attacks.** By associating these web ACLs with AWS WAF, the company can protect its web application from SQL injection attempts without requiring changes to the application code or infrastructure.

解析: To resolve the SQL injection vulnerability, the company should use AWS WAF (Web Application Firewall) in front of the Application Load Balancer (ALB). AWS WAF can be configured with web ACLs that include

rules to detect and block SQL injection attacks. By associating these web ACLs with AWS WAF, the company can protect its web application from SQL injection attempts without requiring changes to the application code or infrastructure.

293. Question #341A 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**?

- 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.

答案: D

解析: To meet the requirements with the least operational overhead, the solutions architect should use a Lake Formation blueprint to ingest the data from the Amazon Aurora MySQL database to the S3 data lake. **AWS Lake Formation can be used to enforce column-level access control for the QuickSight users.** By using Amazon Athena as the data source in QuickSight, the company can create visualizations that join the data lake with the operational data while maintaining security and governance over

the data. This approach leverages the existing AWS Lake Formation governance capabilities and minimizes additional configuration and maintenance.

解析: To meet the requirements with the least operational overhead, the solutions architect should use a Lake Formation blueprint to ingest the data from the Amazon Aurora MySQL database to the S3 data lake. AWS Lake Formation can be used to enforce column-level access control for the QuickSight users. By using Amazon Athena as the data source in QuickSight, the company can create visualizations that join the data lake with the operational data while maintaining security and governance over the data. This approach leverages the existing AWS Lake Formation governance capabilities and minimizes additional configuration and maintenance.

294. Question #342A 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?

- 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%.

答案：C

解析：old(B)→new(C)

old: To automate the capacity provisioning process with the least operational overhead, the solutions architect should create a scheduled scaling policy for the Auto Scaling group. This policy can be configured to set the desired, minimum, and maximum capacity based on the company's requirements and set to recur weekly, starting 30 minutes before the batch jobs run. **This approach does not require ongoing analysis of capacity trends or real-time monitoring of CPU utilization, making it a straightforward and low-maintenance solution.**

new: waiting...

解析：old(B)→new(C)

old: To automate the capacity provisioning process with the least operational overhead, the solutions architect should create a scheduled scaling policy for the Auto Scaling group. This policy can be configured to set the desired, minimum, and maximum capacity based on the company's requirements and set to recur weekly, starting 30 minutes before the batch jobs run. This approach does not require ongoing analysis of capacity trends or real-time monitoring of CPU utilization, making it a straightforward and low-maintenance solution.

new: waiting...

295. Question #343A 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**?

- 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 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.

答案: C

解析: To meet the disaster recovery requirements with the least operational overhead, the solutions architect should migrate the MySQL database to an Amazon Aurora global database. This option allows hosting the primary DB cluster in the primary Region and a secondary DB cluster in the DR Region, providing a multi-region, high-availability, and disaster recovery solution. Aurora global databases are designed to minimize operational complexity and provide automated replication and failover across AWS Regions.

解析: To meet the disaster recovery requirements with the least operational overhead, the solutions architect should migrate the MySQL database to an Amazon Aurora global database. This option allows hosting the primary DB cluster in the primary Region and a secondary DB cluster in the DR Region, providing a multi-region, high-availability, and disaster recovery solution. Aurora global databases are designed to minimize operational complexity and provide automated replication and failover across AWS Regions.

296. Question #344A 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?**

- 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.

答案：A

解析：To allow the Java application to parse messages larger than 256 KB with the fewest changes to the code, the solutions architect should use the **Amazon SQS Extended Client Library for Java**. This library enables the application to send and receive large messages by storing the message payload in Amazon S3 and referencing it in the SQS message. This approach does not require significant changes to the application code and leverages existing SQS integration while overcoming the size limitation.

解析：To allow the Java application to parse messages larger than 256 KB with the fewest changes to the code, the solutions architect should use the **Amazon SQS Extended Client Library for Java**. This library enables the application to send and receive large messages by storing the message payload in Amazon S3 and referencing it in the SQS message. This approach does not require significant changes to the application code and leverages existing SQS integration while overcoming the size limitation.

297. Question #345A 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**?

- A. Use Amazon Cognito for authentication. Use Lambda@Edge 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 Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

答案：A

解析：To implement a serverless, globally distributed, and cost-effective solution for authentication and authorization with low login latency, the solutions architect should use Amazon Cognito for handling user authentication, Lambda@Edge for executing authorization logic at the edge of the network closest to the users, and Amazon CloudFront for serving web content globally. This combination provides a scalable and serverless architecture that can grow with the user base while maintaining low latency and reducing operational costs.

解析：To implement a serverless, globally distributed, and cost-effective solution for authentication and authorization with low login latency, the solutions architect should use Amazon Cognito for handling user authentication, Lambda@Edge for executing authorization logic at the edge of the network closest to the users, and Amazon CloudFront for serving web content globally. This combination provides a scalable and serverless architecture that can grow with the user base while maintaining low latency and reducing operational costs.

298. Question #346A 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?

- A. Volume Gateway
- B. Tape Gateway
- C. Amazon FSx File Gateway
- D. Amazon S3 File Gateway

答案: D

解析: To migrate the data to Amazon S3 while maintaining the same look and feel for the client workstations, the solutions architect should provision an Amazon S3 File Gateway. This type of Storage Gateway provides file system interface access to objects stored in S3, supporting both SMB and NFS protocols, which allows client workstations to interact with the data as if it were stored on a traditional NAS device.

Additionally, S3 Lifecycle policies can be used to manage the data, transitioning it to more cost-effective storage classes over time for the inactive data.

解析: To migrate the data to Amazon S3 while maintaining the same look and feel for the client workstations, the solutions architect should provision an Amazon S3 File Gateway. This type of Storage Gateway provides file system interface access to objects stored in S3, supporting both SMB and NFS protocols, which allows client workstations to interact with the data as if it were stored on a traditional NAS device.

Additionally, S3 Lifecycle policies can be used to manage the data, transitioning it to more cost-effective storage classes over time for the inactive data.

299. Question #347A 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?

- A. Compute Savings Plan
- B. EC2 Instance Savings Plan
- C. Zonal Reserved Instances
- D. Standard Reserved Instances

答案: A

解析: To maximize cost savings while maintaining the flexibility to change instance family and sizes, the solutions architect should choose the Compute Savings Plan. This plan offers significant savings on compute usage for Amazon EC2 and AWS Lambda, and it allows for changes to instance types within the same instance family. Unlike EC2 Instance Savings Plans, Compute Savings Plans provide this flexibility without being locked into a specific instance size, making it the most cost-effective and flexible option for the company's needs.

解析: To maximize cost savings while maintaining the flexibility to change instance family and sizes, the solutions architect should choose the Compute Savings Plan. This plan offers significant savings on compute usage for Amazon EC2 and AWS Lambda, and it allows for changes to instance types within the same instance family. Unlike EC2 Instance Savings Plans, Compute Savings Plans provide this flexibility without being locked into a specific instance size, making it the most cost-effective and flexible option for the company's needs.

300. Question #348A 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?

- A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA).

- 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.

答案: B

解析: Given that the data workload is constant and predictable, using provisioned mode with specified read and write capacity units (RCUs and WCUs) is the most cost-effective solution. This allows the company to pay for the exact capacity needed without incurring the additional costs associated with on-demand mode or the unnecessary expense of over-provisioning. DynamoDB Standard-IA is designed for infrequent access and would not be suitable for a workload that is constant and predictable.

解析: Given that the data workload is constant and predictable, using provisioned mode with specified read and write capacity units (RCUs and WCUs) is the most cost-effective solution. This allows the company to pay for the exact capacity needed without incurring the additional costs associated with on-demand mode or the unnecessary expense of over-provisioning. DynamoDB Standard-IA is designed for infrequent access and would not be suitable for a workload that is constant and predictable.

301. Question #349A 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?

- 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.

答案：B

解析：To securely share an encrypted database snapshot with the acquiring company's AWS account, the solutions architect should create a database snapshot and then add the acquiring company's AWS account to the policy of the AWS KMS customer managed key that is used to encrypt the snapshot. This allows the acquiring company to access and decrypt the shared snapshot using the same KMS key. It is important to maintain encryption throughout the process to protect the confidential data.

解析：To securely share an encrypted database snapshot with the acquiring company's AWS account, the solutions architect should create a database snapshot and then add the acquiring company's AWS account to the policy of the AWS KMS customer managed key that is used to encrypt the snapshot. This allows the acquiring company to access and decrypt the shared snapshot using the same KMS key. It is important to maintain encryption throughout the process to protect the confidential data.

302. Question #351A 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?

- 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.

答案: D

解析: To create an event-driven, serverless, and distributed architecture with minimal operational overhead, the solutions architect should build out the workflow in AWS Step Functions and use it to create a state machine. This state machine can then invoke AWS Lambda functions to process the different steps of the workflow. AWS Step Functions manage the operational aspects of the workflow, and AWS Lambda provides serverless compute for the workflow steps, ensuring a scalable and event-driven architecture.

解析: To create an event-driven, serverless, and distributed architecture with minimal operational overhead, the solutions architect should build out the workflow in AWS Step Functions and use it to create a state machine. This state machine can then invoke AWS Lambda functions to process the different steps of the workflow. AWS Step Functions manage the operational aspects of the workflow, and AWS Lambda provides serverless compute for the workflow steps, ensuring a scalable and event-driven architecture.

303. Question #352A 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?

- A. Set up 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.

答案：B

解析：To minimize latency and packet loss for an online multiplayer game that uses UDP, the solutions architect should set up AWS Global Accelerator with UDP listeners. Global Accelerator is designed to improve the availability and performance of applications that use UDP by routing traffic through the optimal AWS edge location to the game servers. This ensures that players are connected to the nearest endpoint for the best gaming experience.

解析：To minimize latency and packet loss for an online multiplayer game that uses UDP, the solutions architect should set up AWS Global Accelerator with UDP listeners. Global Accelerator is designed to improve the availability and performance of applications that use UDP by routing traffic through the optimal AWS edge location to the game servers. This ensures that players are connected to the nearest endpoint for the best gaming experience.

304. Question #353A 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. Which solution will meet these requirements MOST cost-effectively?
- 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.

答案：B

解析：To achieve cost-effectiveness while maintaining performance and the ability to handle double the IOPS, the solutions architect should migrate to a Multi-AZ deployment of Amazon RDS for MySQL with a General Purpose SSD (gp2) EBS volume. RDS provides a managed database service that can handle failover and automatic scaling, and gp2 volumes can automatically scale up to 3,000 IOPS for every 1 TB of storage, which is cost-effective and provides the required performance without the need for manual intervention.

解析：To achieve cost-effectiveness while maintaining performance and the ability to handle double the IOPS, the solutions architect should migrate to a Multi-AZ deployment of Amazon RDS for MySQL with a General Purpose SSD (gp2) EBS volume. RDS provides a managed database service that can handle failover and automatic scaling, and gp2 volumes can automatically scale up to 3,000 IOPS for every 1 TB of storage, which is cost-effective and provides the required performance without the need for manual intervention.

305. Question #354A 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?
- 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.

答案：B

解析：To reduce application failures caused by database connection timeouts with minimal code changes, the solutions architect should enable RDS Proxy on the RDS DB instance. RDS Proxy can manage database connections more efficiently, providing a scalable and resilient connection management solution that can handle sudden increases in traffic without the need to modify the application code.

解析：To reduce application failures caused by database connection timeouts with minimal code changes, the solutions architect should enable RDS Proxy on the RDS DB instance. RDS Proxy can manage database connections more efficiently, providing a scalable and resilient connection management solution that can handle sudden increases in traffic without the need to modify the application code.

306. Question #355A 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**?

- 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.

答案：D

解析：Given the CPU and memory requirements of the batch job, AWS Batch on Amazon EC2 is the most suitable solution for running the job within 15 minutes with minimal operational overhead. **AWS Batch can manage the batch jobs, leveraging the compute capacity of EC2 instances**, which can be sized appropriately to meet the vCPU and memory needs of the job. This approach does not require changes to the application and can handle the batch processing efficiently.

解析：Given the CPU and memory requirements of the batch job, AWS Batch on Amazon EC2 is the most suitable solution for running the job within 15 minutes with minimal operational overhead. **AWS Batch can manage the batch**

jobs, leveraging the compute capacity of EC2 instances, which can be sized appropriately to meet the vCPU and memory needs of the job. This approach does not require changes to the application and can handle the batch processing efficiently.

307. Question #356A 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?

- 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.

答案：B

解析：To maintain high availability and resiliency while minimizing storage costs for data that is rarely accessed after 30 days, the solutions architect should move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days. S3 Standard-IA is designed for data that is infrequently accessed but requires rapid access when needed, and it offers lower storage costs compared to S3 Standard while providing the same durability and availability.

解析：To maintain high availability and resiliency while minimizing storage costs for data that is rarely accessed after 30 days, the solutions architect should move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days. S3 Standard-IA is designed for data that is infrequently accessed but requires rapid access when needed, and it offers lower storage costs compared to S3 Standard while providing the same durability and availability.

308. Question #358A 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**?

- 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 Lambda@Edge function with an external image management library. Associate the Lambda@Edge 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.

答案: C

解析: To dynamically resize images and serve appropriate formats with the least operational overhead, the solutions architect should use a Lambda@Edge function with an external image management library.

Lambda@Edge can be triggered by CloudFront events and run the image processing code close to the end-users, reducing latency. By associating the Lambda@Edge function with CloudFront behaviors, the images can be resized and formatted on-the-fly as they are requested by clients, without the need for changes to the EC2 instances or additional policies.

解析: To dynamically resize images and serve appropriate formats with the least operational overhead, the solutions architect should use a Lambda@Edge function with an external image management library.

Lambda@Edge can be triggered by CloudFront events and run the image processing code close to the end-users, reducing latency. By associating the Lambda@Edge function with CloudFront behaviors, the images can be resized and formatted on-the-fly as they are requested by clients,

without the need for changes to the EC2 instances or additional policies.

309. Question #359A 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?

- 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.

答案: C

解析: To meet the hospital's requirements, the solutions architect should use the `aws:SecureTransport` condition on S3 bucket policies to ensure all connections to the S3 bucket are encrypted in transit over HTTPS (TLS). Additionally, configuring the S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS) and assigning the compliance team to manage those KMS keys ensures that the PHI data is encrypted at rest and that the compliance team has administrative control over the encryption keys, as required.

解析: To meet the hospital's requirements, the solutions architect should use the aws:SecureTransport condition on S3 bucket policies to ensure all connections to the S3 bucket are encrypted in transit over HTTPS (TLS). Additionally, configuring the S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS) and assigning the compliance team to manage those KMS keys ensures that the PHI data is encrypted at rest and that the compliance team has administrative control over the encryption keys, as required.

310. Question #360A 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?**

- 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.

答案: B

解析: To ensure that the communication between the BuyStock and CheckFunds RESTful web services occurs within the VPC with the fewest changes to the code, the solutions architect should use an interface endpoint for Amazon API Gateway. Interface endpoints are VPC endpoints that allow traffic to flow between the VPC and AWS services without the need to use public internet routes. This approach does not require additional components like an SQS queue or changes to the authorization process and thus minimizes code changes.

解析: To ensure that the communication between the BuyStock and CheckFunds RESTful web services occurs within the VPC with the fewest

changes to the code, the solutions architect should use an interface endpoint for Amazon API Gateway. Interface endpoints are VPC endpoints that allow traffic to flow between the VPC and AWS services without the need to use public internet routes. This approach does not require additional components like an SQS queue or changes to the authorization process and thus minimizes code changes.

311. Question #361A company hosts a **multiplayer gaming application** on AWS. The application 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**?

- 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.

答案: C

解析: To achieve sub-millisecond latency for frequently accessed data and the ability to run one-time queries on historical data with minimal operational overhead, the solutions architect should use Amazon DynamoDB with DynamoDB Accelerator (DAX). **DAX is a fully managed, in-memory caching service that provides fast access to DynamoDB data**. For historical data analysis, exporting data to Amazon S3 and using Amazon Athena to run one-time queries is a cost-effective and scalable approach.

This combination leverages the strengths of both services to meet the performance and analytical requirements.

解析: To achieve sub-millisecond latency for frequently accessed data and the ability to run one-time queries on historical data with minimal operational overhead, the solutions architect should use Amazon DynamoDB with DynamoDB Accelerator (DAX). DAX is a fully managed, in-memory caching service that provides fast access to DynamoDB data. For historical data analysis, exporting data to Amazon S3 and using Amazon Athena to run one-time queries is a cost-effective and scalable approach. This combination leverages the strengths of both services to meet the performance and analytical requirements.

312. Question #363A 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?

- 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

答案: B

解析: To meet the requirement of sending unique events to separate services concurrently while guaranteeing the order of the events, the solutions architect should use Amazon SNS FIFO topics. SNS FIFO topics ensure that each message is received by subscribers in the same order that it was published. This is critical for applications like a game system where the order of events is important for consistent system state across different services.

解析: To meet the requirement of sending unique events to separate services concurrently while guaranteeing the order of the events, the solutions architect should use Amazon SNS FIFO topics. SNS FIFO topics ensure that each message is received by subscribers in the same order that it was published. This is critical for applications like a game

system where the order of events is important for consistent system state across different services.

313. Question #365A 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?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

答案: C

解析: To meet the requirement of being able to restore the database to its state from 5 minutes before any change within the last 30 days, the solutions architect should include the feature of Automated backups in the design. Amazon RDS automated backups allow you to recover your database to any second during the retention period of the backups, which is a default of 7 days but can be extended to 35 days. This feature is crucial for point-in-time recovery and aligns with the company's need for data recovery from accidental changes.

解析: To meet the requirement of being able to restore the database to its state from 5 minutes before any change within the last 30 days, the solutions architect should include the feature of Automated backups in the design. **Amazon RDS automated backups allow you to recover your database to any second during the retention period of the backups**, which is a default of 7 days but can be extended to 35 days. This feature is crucial for point-in-time recovery and aligns with the company's need for data recovery from accidental changes.

314. Question #366A 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?

- 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.

答案：D

解析：To implement access control with the least operational overhead, the solutions architect should use Amazon API Gateway's API usage plans and API keys. This feature allows the creation of different plans that can be associated with API keys, which can then be distributed to users. Users with a valid API key that corresponds to a plan granting access to premium content will be allowed to access the premium features of the application. This approach centralizes access control at the API Gateway level and avoids the need for fine-grained permissions at the database level or additional filtering with AWS WAF.

解析：To implement access control with the least operational overhead, the solutions architect should use Amazon API Gateway's API usage plans and API keys. This feature allows the creation of different plans that can be associated with API keys, which can then be distributed to users. Users with a valid API key that corresponds to a plan granting access to premium content will be allowed to access the premium features of the application. This approach centralizes access control at the API Gateway level and avoids the need for fine-grained permissions at the database level or additional filtering with AWS WAF.

315. Question #367A 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?

- 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.

答案: A

解析: To improve the performance and availability of the UDP-based application while adhering to the compliance requirements that mandate on-premises hosting, the solutions architect should configure Network Load Balancers (NLBs) in the three AWS Regions. These NLBs will be connected to the on-premises endpoints. By creating an accelerator with

AWS Global Accelerator and registering the NLBs as its endpoints, the architect can utilize Global Accelerator's traffic routing capabilities to direct users to the nearest endpoint. This setup enhances the application's performance and availability without violating the on-premises hosting mandate.

解析：To improve the performance and availability of the UDP-based application while adhering to the compliance requirements that mandate on-premises hosting, the solutions architect should configure Network Load Balancers (NLBs) in the three AWS Regions. These NLBs will be connected to the on-premises endpoints. By creating an accelerator with AWS Global Accelerator and registering the NLBs as its endpoints, the architect can utilize Global Accelerator's traffic routing capabilities to direct users to the nearest endpoint. This setup enhances the application's performance and availability without violating the on-premises hosting mandate.

316. Question #368A 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?

- 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.

答案：A

解析：To ensure that all new IAM users in the AWS account adhere to specific password complexity requirements and mandatory rotation periods, the solutions architect should set an overall password policy for the entire AWS account. AWS allows the creation of an account password policy that applies to all IAM users, which can define the required password length, complexity, and expiration period.

解析：To ensure that all new IAM users in the AWS account adhere to specific password complexity requirements and mandatory rotation periods, the solutions architect should set an overall password policy for the

entire AWS account. AWS allows the creation of an account password policy that applies to all IAM users, which can define the required password length, complexity, and expiration period.

317. Question #369A 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 with the LEAST operational overhead.

- 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.

答案：A

解析：To address the concerns of performance and scalability with the least operational overhead, the solutions architect should use AWS Batch to run the tasks as jobs. AWS Batch is designed to run batch computing workloads on AWS and can manage the scheduling and execution of the tasks without the need for containerization or the creation of Lambda functions. By using Amazon EventBridge (formerly Amazon CloudWatch Events), the tasks can be scheduled to run at specific times or intervals, allowing for efficient resource utilization and scalability.

解析：To address the concerns of performance and scalability with the least operational overhead, the solutions architect should use AWS Batch to run the tasks as jobs. AWS Batch is designed to run batch computing workloads on AWS and can manage the scheduling and execution of the tasks without the need for containerization or the creation of Lambda

functions. By using Amazon EventBridge (formerly Amazon CloudWatch Events), the tasks can be scheduled to run at specific times or intervals, allowing for efficient resource utilization and scalability.

318. Question #370A 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?

- 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.

答案：C

解析：To meet the requirement for a managed solution that allows private subnet EC2 instances to communicate with a license server over the internet while minimizing operational maintenance, the solutions architect should provision a NAT gateway in a public subnet. NAT gateways are managed services that reduce the operational overhead associated with setting up and maintaining a NAT instance. By modifying each private subnet's route table to use the NAT gateway, the EC2 instances can access the internet without requiring additional configuration or maintenance.

解析：To meet the requirement for a managed solution that allows private subnet EC2 instances to communicate with a license server over the internet while minimizing operational maintenance, the solutions architect should provision a NAT gateway in a public subnet. NAT gateways are managed services that reduce the operational overhead associated with

setting up and maintaining a NAT instance. By modifying each private subnet's route table to use the NAT gateway, the EC2 instances can access the internet without requiring additional configuration or maintenance.

319. Question #372A 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**?

- 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.

答案：B

解析：The most cost-effective solution for storing high-resolution GIS images that require high availability and scalability during frequent updates is to store the images in Amazon S3 buckets (Option B). S3 is optimized for storing large amounts of data and can handle the frequent updates and retrievals that occur during a natural disaster. Using Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value allows for quick access and retrieval of the images using the geographic code. This combination leverages the strengths of both services to provide a scalable and cost-effective solution.

解析：The most cost-effective solution for storing high-resolution GIS images that require high availability and scalability during frequent updates is to store the images in Amazon S3 buckets (Option B). S3 is

optimized for storing large amounts of data and can handle the frequent updates and retrievals that occur during a natural disaster. Using Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value allows for quick access and retrieval of the images using the geographic code. This combination leverages the strengths of both services to provide a scalable and cost-effective solution.

320. Question #373A 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?

- 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

答案: D

解析: The most cost-effective storage solution for the company's requirements is to use the S3 Standard storage class initially for frequent access needs (Option D). After 30 days, when the data access pattern becomes less frequent, the S3 Lifecycle policy can transition the data to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class.

Finally, after 1 year, the data can be moved to S3 Glacier Deep Archive for long-term archival storage. This tiered approach ensures that the data is stored in the most cost-effective storage class based on access patterns while still being readily available for ML model training and analysis.

解析: The most cost-effective storage solution for the company's requirements is to use the S3 Standard storage class initially for frequent access needs (Option D). After 30 days, when the data access pattern becomes less frequent, the S3 Lifecycle policy can transition the data to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Finally, after 1 year, the data can be moved to S3 Glacier Deep Archive for long-term archival storage. This tiered approach ensures that the data is stored in the most cost-effective storage class based on access patterns while still being readily available for ML model training and analysis.

321. Question #374A 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?

- 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.

答案: D

解析: To maximize cost-effectiveness for network connectivity between multiple VPCs and an on-premises data center, the solutions architect should set up one AWS Direct Connect connection (Option D). By creating a transit gateway and attaching each VPC to it, the architect can establish a single, central connection point for all VPCs. This setup reduces the overall number of connections needed and leverages the transit gateway to route traffic between the VPCs and the on-premises data center, resulting in a more efficient and cost-effective network architecture.

解析: To maximize cost-effectiveness for network connectivity between multiple VPCs and an on-premises data center, the solutions architect should set up one AWS Direct Connect connection (Option D). By creating a transit gateway and attaching each VPC to it, the architect can establish a single, central connection point for all VPCs. This setup reduces the overall number of connections needed and leverages the transit gateway to route traffic between the VPCs and the on-premises data center, resulting in a more efficient and cost-effective network architecture.

322. Question #375An 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**?

- 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.

答案：A

解析：To design an architecture that combines multiple AWS Lambda functions into responsive serverless applications with the least operational overhead, the solutions architect should use AWS Step Functions (Option A). Step Functions is a serverless workflow service that coordinates multiple AWS services, including Lambda, into serverless applications. It provides a visual interface to define, monitor, and debug application workflows, making it an ideal choice for orchestrating complex workflows that involve manual approvals and interactions with various AWS services and resources.

解析：To design an architecture that combines multiple AWS Lambda functions into responsive serverless applications with the least operational overhead, the solutions architect should use AWS Step Functions (Option A). Step Functions is a serverless workflow service that coordinates multiple AWS services, including Lambda, into serverless applications. It provides a visual interface to define, monitor, and debug application workflows, making it an ideal choice for orchestrating complex workflows that involve manual approvals and interactions with various AWS services and resources.

323. Question #376A 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**?

- 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.

答案：A

解析：To resolve database connection rejection errors with the least operational overhead, the solutions architect should create a proxy in RDS Proxy (Option A). RDS Proxy is designed to manage database connections and can handle a large number of connections from serverless applications. By configuring the applications to use the DB instance through RDS Proxy, the company can alleviate connection pressure during high demand periods without the need to change the database instance class or manage additional services like ElastiCache.

解析：To resolve database connection rejection errors with the least operational overhead, the solutions architect should create a proxy in RDS Proxy (Option A). RDS Proxy is designed to manage database connections and can handle a large number of connections from serverless applications. By configuring the applications to use the DB instance through RDS Proxy, the company can alleviate connection pressure during high demand periods without the need to change the database instance class or manage additional services like ElastiCache.

324. Question #377A 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?

- 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.

答案：B

解析：The most efficient solution for ensuring that EC2 instances send reports to the auditing system upon launch and termination is to use EC2 Auto Scaling lifecycle hooks (Option B). Lifecycle hooks allow you to perform actions on instances as they launch or terminate, such as running a custom script to send data to the audit system. This approach is more efficient than using a scheduled Lambda function, which would require periodic execution and may not capture all instances in time. It also avoids the need for manual configuration through user data or operating system scripts.

解析：The most efficient solution for ensuring that EC2 instances send reports to the auditing system upon launch and termination is to use EC2 Auto Scaling lifecycle hooks (Option B). Lifecycle hooks allow you to perform actions on instances as they launch or terminate, such as running a custom script to send data to the audit system. This approach is more efficient than using a scheduled Lambda function, which would require periodic execution and may not capture all instances in time. It also avoids the need for manual configuration through user data or operating system scripts.

325. Question #378A 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?

- 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.

答案：B

解析：For a real-time multiplayer game that requires UDP support and the ability to handle non-relational data, the solutions architect should recommend using a Network Load Balancer (NLB) for traffic distribution and Amazon DynamoDB on-demand for data storage (Option B). NLB supports UDP traffic, which is essential for real-time gaming, and can handle the anticipated spikes in demand. DynamoDB on-demand provides a scalable and serverless database solution that automatically adjusts to the workload, making it ideal for storing gamer scores and other non-relational data without the need for manual intervention.

解析：For a real-time multiplayer game that requires UDP support and the ability to handle non-relational data, the solutions architect should recommend using a Network Load Balancer (NLB) for traffic distribution and Amazon DynamoDB on-demand for data storage (Option B). NLB supports UDP traffic, which is essential for real-time gaming, and can handle the anticipated spikes in demand. DynamoDB on-demand provides a scalable and serverless database solution that automatically adjusts to the workload, making it ideal for storing gamer scores and other non-relational data without the need for manual intervention.

326. Question #379A 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?

- 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.

答案：B

解析：To minimize response latency with the fewest changes, the solutions architect should configure provisioned concurrency for the Lambda function (Option B). Provisioned concurrency ensures that a specified number of Lambda instances are always ready to respond to incoming requests, reducing the "cold start" latency that occurs when a new instance is initialized. This approach does not require changes to the database configuration or the frontend application and is the most efficient solution for improving response times in this scenario.

解析：To minimize response latency with the fewest changes, the solutions architect should configure provisioned concurrency for the Lambda function (Option B). Provisioned concurrency ensures that a specified number of Lambda instances are always ready to respond to incoming requests, reducing the "cold start" latency that occurs when a new instance is initialized. This approach does not require changes to the database configuration or the frontend application and is the most efficient solution for improving response times in this scenario.

327. Question #380A 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?

- 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.

答案: D

解析: To automatically start and stop EC2 instances and DB instances outside of business hours while minimizing cost and infrastructure maintenance, the solutions architect should create an AWS Lambda function (Option D). The Lambda function can be designed to start and stop the instances according to a predefined schedule. By configuring Amazon EventBridge to invoke this Lambda function on a schedule, the company can achieve automated management of its instances without the need for additional EC2 instances or third-party solutions. This approach is both cost-effective and reduces the operational overhead associated with managing the instances.

解析: To automatically start and stop EC2 instances and DB instances outside of business hours while minimizing cost and infrastructure maintenance, the solutions architect should create an AWS Lambda function (Option D). The Lambda function can be designed to start and stop the instances according to a predefined schedule. By configuring Amazon EventBridge to invoke this Lambda function on a schedule, the company can achieve automated management of its instances without the need for additional EC2 instances or third-party solutions. This approach is both cost-effective and reduces the operational overhead associated with managing the instances.

328. Question #381A 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 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?

- 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.

答案：B

解析：To speed up the reporting process with the least amount of change to the application code, the solutions architect should set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica (Option B). By issuing queries to the Aurora Replica, the reporting process can be offloaded from the primary database instance, which allows the primary instance to handle new document modifications and additions without impact. This approach leverages the existing PostgreSQL compatibility and minimizes the need for changes to the application code.

解析：To speed up the reporting process with the least amount of change to the application code, the solutions architect should set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica (Option B). By issuing queries to the Aurora Replica, the reporting process can be offloaded from the primary database instance, which allows the primary instance to handle new document modifications and additions

without impact. This approach leverages the existing PostgreSQL compatibility and minimizes the need for changes to the application code.

329. Question #382A 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?

- 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 using AWS Key Management Service (AWS KMS).

答案：A

解析：To improve the security of the data in transit, the solutions architect should configure a TLS listener and deploy the server certificate on the Network Load Balancer (Option A). This ensures that the data transmitted between the NLB and the EC2 instances is encrypted, providing a secure channel for communication. While AWS Shield Advanced and AWS WAF can provide additional security benefits, they are not directly related to encrypting data in transit. Encrypting the Amazon EBS volume using AWS KMS, as mentioned in Option D, secures data at rest rather than in transit.

解析：To improve the security of the data in transit, the solutions architect should configure a TLS listener and deploy the server certificate on the Network Load Balancer (Option A). This ensures that the data transmitted between the NLB and the EC2 instances is encrypted, providing a secure channel for communication. While AWS Shield Advanced and AWS WAF can provide additional security benefits, they are not directly related to encrypting data in transit. Encrypting the Amazon EBS volume using AWS KMS, as mentioned in Option D, secures data at rest rather than in transit.

330. Question #383A 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?

- A. Dedicated Reserved Hosts
- B. Dedicated On-Demand Hosts
- C. Dedicated Reserved Instances
- D. Dedicated On-Demand Instances

答案：A

解析：Given that the company has existing licenses based on sockets and cores, and they are looking for a predictable capacity and uptime, the most cost-effective Amazon EC2 pricing option would be Dedicated Reserved Hosts (Option A). This option allows the company to use their existing licenses while benefiting from the cost savings of reserved instances. It also provides the necessary dedicated physical resources required by the off-the-shelf application.

解析：Given that the company has existing licenses based on sockets and cores, and they are looking for a predictable capacity and uptime, the most cost-effective Amazon EC2 pricing option would be Dedicated Reserved Hosts (Option A). This option allows the company to use their existing licenses while benefiting from the cost savings of reserved instances. It also provides the necessary dedicated physical resources required by the off-the-shelf application.

331. Question #384A 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?**

- 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).

答案: C

解析: The most cost-effective solution that meets the requirements of high availability, POSIX compliance, maximum data durability, and shareability across EC2 instances is to use the Amazon Elastic File System (EFS) Standard storage class (Option C). EFS is designed to provide these capabilities and can be accessed by multiple EC2 instances simultaneously. By creating a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access, the company can also optimize costs for data that is less frequently used after the initial 30 days.

解析: The most cost-effective solution that meets the requirements of high availability, POSIX compliance, maximum data durability, and shareability across EC2 instances is to use the Amazon Elastic File System (EFS) Standard storage class (Option C). EFS is designed to provide these capabilities and can be accessed by multiple EC2 instances simultaneously. By creating a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access, the company can also optimize costs for data that is less frequently used after the initial 30 days.

332. Question #385A 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?

- 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.

答案: C

解析: To adhere to the company policy of least privilege access, the solutions architect should create a security group for the web servers and configure it to allow traffic on port 443 only from the security group associated with the load balancer (Option C). This ensures that only the load balancer can communicate with the web servers on HTTPS. Additionally, a security group for the MySQL servers should be created, allowing traffic on port 3306 only from the security group of the web servers. This ensures that only the web servers can access the MySQL servers, which is necessary for the application architecture and maintains the principle of least privilege.

解析: To adhere to the company policy of least privilege access, the solutions architect should create a security group for the web servers and configure it to allow traffic on port 443 only from the security group associated with the load balancer (Option C). This ensures that only the load balancer can communicate with the web servers on HTTPS.

Additionally, a security group for the MySQL servers should be created, allowing traffic on port 3306 only from the security group of the web servers. This ensures that only the web servers can access the MySQL servers, which is necessary for the application architecture and maintains the principle of least privilege.

333. Question #386 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?

- 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.

答案：B

解析：To improve the performance of the backend and reduce the impact of frequent calls to the database that return identical datasets, the solutions architect should implement Amazon ElastiCache (Option B).

ElastiCache, specifically using Redis or Memcached, can be used to cache these datasets, thereby reducing the need to repeatedly query the database. This approach minimizes latency and improves application response times by serving data from the cache instead of the database.

解析：To improve the performance of the backend and reduce the impact of frequent calls to the database that return identical datasets, the solutions architect should implement Amazon ElastiCache (Option B).

ElastiCache, specifically using Redis or Memcached, can be used to cache these datasets, thereby reducing the need to repeatedly query the database. This approach minimizes latency and improves application response times by serving data from the cache instead of the database.

334. Question #388A 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?

- 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 tier's security group.

答案: D

解析: Since the network ACLs, security groups, and route tables are in their default states, the issue is likely related to security group rules. The solutions architect should recommend adding an inbound rule to the security group of the database tier's RDS instance (Option D). This rule should allow traffic from the security group associated with the web tier's EC2 instances. By doing so, the web tier will be able to communicate with the database tier, resolving the connectivity issue.

解析: Since the network ACLs, security groups, and route tables are in their default states, the issue is likely related to security group rules. The solutions architect should recommend adding an inbound rule to the security group of the database tier's RDS instance (Option D). This rule should allow traffic from the security group associated with the web tier's EC2 instances. By doing so, the web tier will be able to communicate with the database tier, resolving the connectivity issue.

335. Question #389A 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?

- 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.

答案：A

解析：To ensure that business reporting queries do not impact the write operations to the production DB instance, the solutions architect should deploy RDS read replicas (Option A). Read replicas can handle the read load, such as reporting queries, while the primary instance manages write operations. This approach allows for scaling the read workload without affecting the performance of the primary instance.

解析：To ensure that business reporting queries do not impact the write operations to the production DB instance, the solutions architect should deploy RDS read replicas (Option A). Read replicas can handle the read load, such as reporting queries, while the primary instance manages write operations. This approach allows for scaling the read workload without affecting the performance of the primary instance.

336. Question #391A 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?

- 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.

答案: C

解析: The correct solution is C because it optimizes the backup strategy for a stateless web application running on EC2 instances in an Auto Scaling group. Since the application is stateless and does not require local storage on the EC2 instances, there is no need to take frequent snapshots of the EBS volumes. Instead, retaining the latest AMIs of the web and application tiers ensures that the application can be quickly scaled and restored without the need for frequent EBS snapshots. For the database layer, enabling automated backups in Amazon RDS and using point-in-time recovery allows the company to meet its RPO of 2 hours efficiently. This approach maximizes scalability and optimizes resource utilization by focusing on the most critical components of the application infrastructure.

解析: The correct solution is C because it optimizes the backup strategy for a stateless web application running on EC2 instances in an Auto Scaling group. Since the application is stateless and does not require local storage on the EC2 instances, there is no need to take frequent snapshots of the EBS volumes. Instead, retaining the latest AMIs of the web and application tiers ensures that the application can be quickly scaled and restored without the need for frequent EBS snapshots. For the database layer, enabling automated backups in Amazon RDS and using

point-in-time recovery allows the company to meet its RPO of 2 hours efficiently. This approach maximizes scalability and optimizes resource utilization by focusing on the most critical components of the application infrastructure.

337. Question #392A 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?

- 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.

答案: A

解析: To make the web application secure and accessible to global customers with dynamic IP addresses, the solutions architect should configure the security group for the web servers to allow inbound traffic on port 443 from **anywhere (0.0.0.0/0)** (Option A). This ensures that the web tier is publicly accessible via HTTPS. For the database tier, the security group should be configured to allow inbound traffic on port 3306

only from the security group associated with the web servers. This restricts database access to the web tier, enhancing security by not exposing the database directly to the internet.

解析: To make the web application secure and accessible to global customers with dynamic IP addresses, the solutions architect should configure the security group for the web servers to allow inbound traffic on port 443 from anywhere (0.0.0.0/0) (Option A). This ensures that the web tier is publicly accessible via HTTPS. For the database tier, the security group should be configured to allow inbound traffic on port 3306 only from the security group associated with the web servers. This restricts database access to the web tier, enhancing security by not exposing the database directly to the internet.

338. Question #393A 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?

- 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.

答案: C

解析: To capture text from audio files and remove personally identifiable information (PII), the solutions architect should configure an Amazon

Transcribe transcription job with PII redaction enabled (Option C). When an audio file is uploaded to the S3 bucket, an AWS Lambda function can be triggered to start the transcription job, which will transcribe the audio to text and redact the PII. The resulting text without PII can then be stored in a separate S3 bucket, ensuring that the customer's data is protected.

解析: To capture text from audio files and remove personally identifiable information (PII), the solutions architect should configure an Amazon Transcribe transcription job with PII redaction enabled (Option C). When an audio file is uploaded to the S3 bucket, an AWS Lambda function can be triggered to start the transcription job, which will transcribe the audio to text and redact the PII. The resulting text without PII can then be stored in a separate S3 bucket, ensuring that the customer's data is protected.

339. Question #394A 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?

- 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.

答案: B

解析: Here's why this is the recommended approach: 1. **The current setup uses a gp3 volume, which allows for independent scaling of IOPS and throughput without changing the volume size.** 2. The database

administrator observed performance degradation when read and write IOPS exceed 20,000, indicating that the current IOPS limit is the bottleneck.

3. gp3 volumes provide a baseline of 3,000 IOPS, but can be scaled up to 16,000 IOPS without changing the volume size or type. 4. By increasing the provisioned IOPS on the existing gp3 volume, you can address the performance issue without making significant changes to the infrastructure. To implement this solution:

1. Use the AWS Management Console, CLI, or API to modify the EBS volume settings for the RDS instance.
2. Increase the provisioned IOPS to a value above 20,000 (e.g., 25,000 IOPS) to accommodate the observed peak demand.
3. Monitor the application performance after the change to ensure it meets the required levels.
4. Fine-tune the IOPS setting as needed based on ongoing performance monitoring.

Additional considerations:

- Increasing IOPS on a gp3 volume incurs additional costs, so balance performance needs with budget constraints.
- Regularly review and adjust the IOPS settings based on actual usage patterns to optimize costs.
- Consider implementing read replicas or caching solutions if read performance is a significant factor in the bottleneck.
- Ensure that the EC2 instances hosting the application are appropriately sized to handle the increased database performance.

By following this approach, you can address the performance issues while maintaining the existing infrastructure and minimizing potential disruptions to the application.

Sources

- [1] [EBS volume types – Optimizing MySQL Running on Amazon EC2 Using Amazon EBS] (<https://docs.aws.amazon.com/whitepapers/latest/optimizing-mysql-on-ec2-using-amazon-ebs/ebs-volume-types.html>)
- [3] [Best storage practices for running production workloads on hosted databases with Amazon RDS or Amazon EC2 | AWS Database Blog] (<https://aws.amazon.com/blogs/database/best-storage-practices-for-running-production-workloads-on-hosted-databases-with-amazon-rds-or-amazon-ec2/>)
- [6] [I/O-intensive storage modifications – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.I0Intensive.html)

解析: Here's why this is the recommended approach:

1. The current setup uses a gp3 volume, which allows for independent scaling of IOPS and throughput without changing the volume size.
2. The database

administrator observed performance degradation when read and write IOPS exceed 20,000, indicating that the current IOPS limit is the bottleneck.

3. gp3 volumes provide a baseline of 3,000 IOPS, but can be scaled up to 16,000 IOPS without changing the volume size or type. 4. By increasing the provisioned IOPS on the existing gp3 volume, you can address the performance issue without making significant changes to the infrastructure. To implement this solution:

1. Use the AWS Management Console, CLI, or API to modify the EBS volume settings for the RDS instance.
2. Increase the provisioned IOPS to a value above 20,000 (e.g., 25,000 IOPS) to accommodate the observed peak demand.
3. Monitor the application performance after the change to ensure it meets the required levels.
4. Fine-tune the IOPS setting as needed based on ongoing performance monitoring.

Additional considerations:

- Increasing IOPS on a gp3 volume incurs additional costs, so balance performance needs with budget constraints.
- Regularly review and adjust the IOPS settings based on actual usage patterns to optimize costs.
- Consider implementing read replicas or caching solutions if read performance is a significant factor in the bottleneck.
- Ensure that the EC2 instances hosting the application are appropriately sized to handle the increased database performance.

By following this approach, you can address the performance issues while maintaining the existing infrastructure and minimizing potential disruptions to the application.

Sources

- [1] [EBS volume types – Optimizing MySQL Running on Amazon EC2 Using Amazon EBS] (<https://docs.aws.amazon.com/whitepapers/latest/optimizing-mysql-on-ec2-using-amazon-ebs/ebs-volume-types.html>)
- [3] [Best storage practices for running production workloads on hosted databases with Amazon RDS or Amazon EC2 | AWS Database Blog] (<https://aws.amazon.com/blogs/database/best-storage-practices-for-running-production-workloads-on-hosted-databases-with-amazon-rds-or-amazon-ec2/>)
- [6] [I/O-intensive storage modifications – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.I0Intensive.html)

340. Question #395An 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?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS CloudTrail
- D. AWS Config

答案: C

解析: To find out which IAM user made the configuration changes to the security group rules, the solutions architect should use AWS CloudTrail (Option C). CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. It logs all changes made to resources in an AWS account, including security group changes, allowing the architect to identify the IAM user responsible for the changes.

解析: To find out which IAM user made the configuration changes to the security group rules, the solutions architect should use AWS CloudTrail (Option C). CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. It logs all changes made to resources in an AWS account, including security group changes, allowing the architect to identify the IAM user responsible for the changes.

341. Question #396A 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 AcceleratorThe company wants to protect the solution against DDoS attacks. What should a solutions architect do to meet this requirement?

- 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.

答案：A

解析：To protect the self-managed DNS service against DDoS attacks, the solutions architect should subscribe to AWS Shield Advanced (Option A) and add the AWS Global Accelerator as a resource to protect. AWS Shield Advanced provides additional DDoS protection for AWS resources beyond the automatically provided AWS Shield Standard. Global Accelerator is an AWS resource that can be protected by AWS Shield Advanced, offering enhanced security for the DNS service.

解析：To protect the self-managed DNS service against DDoS attacks, the solutions architect should subscribe to AWS Shield Advanced (Option A) and add the AWS Global Accelerator as a resource to protect. AWS Shield Advanced provides additional DDoS protection for AWS resources beyond the automatically provided AWS Shield Standard. Global Accelerator is an AWS resource that can be protected by AWS Shield Advanced, offering enhanced security for the DNS service.

342. Question #397 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?

- 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.

答案：C

解析：To minimize operational effort for a daily job that can take up to an hour to complete, the solutions architect should create an Amazon ECS cluster with an AWS Fargate launch type (Option C). Fargate is a serverless offering for ECS that abstracts the management of the underlying infrastructure, eliminating the need to provision and manage servers. By using Fargate, the architect can run containerized applications without worrying about the capacity provisioning or scaling. An Amazon EventBridge scheduled event can be set up to trigger the ECS task daily, ensuring that the job runs as required with minimal operational overhead.

解析：To minimize operational effort for a daily job that can take up to an hour to complete, the solutions architect should create an Amazon ECS cluster with an AWS Fargate launch type (Option C). Fargate is a serverless offering for ECS that abstracts the management of the underlying infrastructure, eliminating the need to provision and manage servers. By using Fargate, the architect can run containerized applications without worrying about the capacity provisioning or scaling. An Amazon EventBridge scheduled event can be set up to trigger the ECS task daily, ensuring that the job runs as required with minimal operational overhead.

343. Question #398A 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?

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.

答案：C

解析：Considering the large amount of data (600 TB) that needs to be transferred within a tight deadline of 2 weeks, and the requirement for encryption in transit, the most cost-effective solution is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices (Option C). These devices are designed to facilitate fast and secure data transfers, especially for large volumes of data. The Snowball Edge devices can be shipped to the company, used to transfer the data, and then shipped back to AWS for uploading to Amazon S3, all while maintaining encryption throughout the process.

解析：Considering the large amount of data (600 TB) that needs to be transferred within a tight deadline of 2 weeks, and the requirement for encryption in transit, the most cost-effective solution is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices (Option C). These devices are designed to facilitate fast and secure data transfers, especially for large volumes of data. The Snowball Edge devices can be shipped to the company, used to transfer the data, and then shipped back to AWS for uploading to Amazon S3, all while maintaining encryption throughout the process.

344. Question #399A 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?

- 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 Lambda@Edge 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.

答案：B

解析：To protect the web application from HTTP flood attacks with the least operational overhead, the solutions architect should create a Regional AWS WAF web ACL with a rate-based rule (Option B). This rule can be configured to trigger actions when the number of requests from a user exceeds a certain threshold, helping to mitigate the risk of HTTP flood attacks. Associating the web ACL with the API Gateway stage provides an additional layer of security that is managed by AWS, reducing the operational overhead for the company.

解析：To protect the web application from HTTP flood attacks with the least operational overhead, the solutions architect should create a Regional AWS WAF web ACL with a rate-based rule (Option B). This rule can be configured to trigger actions when the number of requests from a user exceeds a certain threshold, helping to mitigate the risk of HTTP flood attacks. Associating the web ACL with the API Gateway stage provides an additional layer of security that is managed by AWS, reducing the operational overhead for the company.

345. Question #400A 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?

- 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.

答案：C

解析：To meet the requirements with the least amount of operational overhead, the solutions architect should enable Amazon DynamoDB Streams on the table (Option C). DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and can trigger a Lambda function or write to an Amazon SNS topic. By using triggers to write to a single Amazon SNS topic, the architect can notify all internal teams about new weather events without affecting the performance of the current application. This approach is efficient, scalable, and requires minimal changes to the existing infrastructure.

解析：To meet the requirements with the least amount of operational overhead, the solutions architect should enable Amazon DynamoDB Streams on the table (Option C). DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and can trigger a Lambda function or write to an Amazon SNS topic. By using triggers to write to a single Amazon SNS topic, the architect can notify all internal teams about new weather events without affecting the performance of the current application. This approach is efficient, scalable, and requires minimal changes to the existing infrastructure.

346. Question #401A 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?

- 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.

答案: A

解析: To create a highly available and resilient application while avoiding single points of failure and enabling scalability, the solutions architect should deploy the application servers using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones (Option A). Additionally, using an Amazon RDS DB instance in a Multi-A Z configuration ensures that the database layer is also highly available and can survive the failure of a single Availability Zone. This approach provides redundancy, automatic failover, and the ability to scale out to

meet user demand.

解析: To create a highly available and resilient application while avoiding single points of failure and enabling scalability, the solutions architect should deploy the application servers using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones (Option A). Additionally, using an Amazon RDS DB instance in a Multi-AZ configuration ensures that the database layer is also highly available and can survive the failure of a single Availability Zone. This approach provides redundancy, automatic failover, and the ability to scale out to meet user demand.

347. Question #402A 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?

- 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.

答案: C

解析: If Amazon S3 is not receiving all the data sent to Kinesis Data Streams, it could be due to the throughput capacity of the stream being exceeded. To resolve this issue, the solutions architect should update the number of Kinesis shards (Option C). Each shard provides a certain amount of throughput, and by increasing the number of shards, the stream can handle more data, ensuring that all the application's data is

ingested and eventually written to the S3 bucket.

解析: If Amazon S3 is not receiving all the data sent to Kinesis Data Streams, it could be due to the throughput capacity of the stream being exceeded. To resolve this issue, the solutions architect should update the number of Kinesis shards (Option C). Each shard provides a certain amount of throughput, and by increasing the number of shards, the stream can handle more data, ensuring that all the application's data is ingested and eventually written to the S3 bucket.

348. Question #403A 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?

- 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.

答案: D

解析: To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, the solutions architect should create an IAM execution role (Option D) with the permissions required to access S3. This role can then be attached to the Lambda function, allowing it to assume the role and perform the S3 operations on behalf of the IAM user. This is a best practice for managing permissions in AWS, as it adheres to the principle of least privilege and avoids embedding credentials within the application code.

解析: To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, the solutions architect should create an IAM execution role (Option D) with the permissions required to access S3.

This role can then be attached to the Lambda function, allowing it to assume the role and perform the S3 operations on behalf of the IAM user. This is a best practice for managing permissions in AWS, as it adheres to the principle of least privilege and avoids embedding credentials within the application code.

349. Question #404A 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?

- 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.

答案: D

解析: To improve the architecture and ensure that all documents are processed, the solutions architect should create an Amazon SQS queue (Option D). By sending the Lambda function invocation requests to the SQS queue, the application can decouple the document upload process from the processing. This allows for better scalability and ensures that even during high loads, such as after a marketing campaign, the documents are queued and processed reliably. Configuring the SQS queue as an event source for Lambda enables asynchronous processing of the documents.

解析: To improve the architecture and ensure that all documents are processed, the solutions architect should create an Amazon SQS queue (Option D). By sending the Lambda function invocation requests to the SQS queue, the application can decouple the document upload process from the processing. This allows for better scalability and ensures that even during high loads, such as after a marketing campaign, the documents are

queued and processed reliably. Configuring the SQS queue as an event source for Lambda enables asynchronous processing of the documents.

350. Question #407A company is implementing a shared storage solution for a **gaming** application that is hosted in the AWS Cloud. The company needs the ability to use **Lustre** clients to access data. The solution must be **fully managed**. Which solution meets these requirements?

- 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 AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. 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.

答案: D

解析: To meet the requirements for a fully managed shared storage solution that supports Lustre clients, the solutions architect should create an Amazon FSx for Lustre file system (Option D). Amazon FSx for Lustre is a high-performance, scalable file system that is optimized for compute-intensive workloads and supports the Lustre client protocol natively. This service is fully managed by AWS, which means that the company can leverage the performance benefits of Lustre without the operational overhead of managing the file system.

解析: To meet the requirements for a fully managed shared storage solution that supports Lustre clients, the solutions architect should create an Amazon FSx for Lustre file system (Option D). Amazon FSx for Lustre is a high-performance, scalable file system that is optimized for compute-intensive workloads and supports the Lustre client protocol natively. This service is fully managed by AWS, which means that the company can leverage the performance benefits of Lustre without the operational overhead of managing the file system.

351. Question #408A 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?

- 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.

答案: B

解析: To minimize latency and provide rapid failover for data transmission from remote devices, the solutions architect should use AWS Global Accelerator (Option B). By creating an NLB in each of the two Regions and setting up the ECS service as the target, the architect can ensure low-latency processing of the UDP data. **Global Accelerator directs traffic to the optimal endpoint based on the location of the user and the health of the endpoints**. Using Amazon ECS with Fargate launch type

provides a serverless compute environment that automatically scales and manages the underlying infrastructure.

解析: To minimize latency and provide rapid failover for data transmission from remote devices, the solutions architect should use AWS Global Accelerator (Option B). By creating an NLB in each of the two Regions and setting up the ECS service as the target, the architect can ensure low-latency processing of the UDP data. Global Accelerator directs traffic to the optimal endpoint based on the location of the user and the health of the endpoints. Using Amazon ECS with Fargate launch type provides a serverless compute environment that automatically scales and manages the underlying infrastructure.

352. Question #409A 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?**

- 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).

答案: C

解析: For migrating a Windows IIS web application that relies on a file share, the most resilient and durable replacement for the on-premises NAS file share is Amazon FSx for Windows File Server (Option C). Amazon FSx for Windows File Server is a fully managed service that provides a high-performance file system that is compatible with Windows Server workloads. It offers high durability and availability, and it can be accessed by Amazon EC2 instances in multiple Availability Zones, making it a suitable choice for a resilient and durable storage solution.

解析: For migrating a Windows IIS web application that relies on a file share, the most resilient and durable replacement for the on-premises NAS file share is Amazon FSx for Windows File Server (Option C). Amazon FSx for Windows File Server is a fully managed service that provides a high-performance file system that is compatible with Windows Server workloads. It offers high durability and availability, and it can be accessed by Amazon EC2 instances in multiple Availability Zones, making it a suitable choice for a resilient and durable storage solution.

353. Question #410A 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 written to the EBS volumes is **encrypted at rest**. Which solution will meet this requirement?

- 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.

答案: B

解析: To ensure that all data written to Amazon EBS volumes is encrypted at rest, the solutions architect should create the EBS volumes as encrypted volumes (Option B). This can be done by enabling encryption when creating the EBS volumes and specifying a KMS key to be used for encryption. By attaching these encrypted EBS volumes to the EC2 instances, the data will be stored in an encrypted form, meeting the company's requirement for data encryption at rest.

解析: To ensure that all data written to Amazon EBS volumes is encrypted at rest, the solutions architect should create the EBS volumes as encrypted volumes (Option B). This can be done by enabling encryption

when creating the EBS volumes and specifying a KMS key to be used for encryption. By attaching these encrypted EBS volumes to the EC2 instances, the data will be stored in an encrypted form, meeting the company's requirement for data encryption at rest.

354. Question #411A 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?

- 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

答案: C

解析: Given the sporadic usage patterns and the need for a cost-effective database platform that does not require modifications to the existing database, the best solution is to use MySQL-compatible Amazon Aurora Serverless (Option C). **Aurora Serverless automatically scales the database's compute resources based on the application's needs, making it a cost-effective choice for workloads with variable usage.** It is also compatible with MySQL, which means that the company can migrate the database to Aurora Serverless without making changes to the database itself.

解析: Given the sporadic usage patterns and the need for a cost-effective database platform that does not require modifications to the existing database, the best solution is to use MySQL-compatible Amazon Aurora Serverless (Option C). **Aurora Serverless automatically scales the database's compute resources based on the application's needs, making it a cost-effective choice for workloads with variable usage.** It is also compatible with MySQL, which means that the company can migrate the

database to Aurora Serverless without making changes to the database itself.

355. Question #412 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?

- 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.

答案: D

解析: To ensure that all S3 objects in the AWS account remain private and to avoid accidental exposure, the most effective solution is to use the S3 Block Public Access feature on the account level (Option D). This feature includes settings that can be applied to all S3 buckets to prevent public access. Additionally, creating a service control policy (SCP) within AWS Organizations and applying it to the account provides a governance structure that prevents IAM users from changing the Block Public Access settings, ensuring a consistent security posture across the account.

解析: To ensure that all S3 objects in the AWS account remain private and to avoid accidental exposure, the most effective solution is to use the S3 Block Public Access feature on the account level (Option D). This

feature includes settings that can be applied to all S3 buckets to prevent public access. Additionally, creating a service control policy (SCP) within AWS Organizations and applying it to the account provides a governance structure that prevents IAM users from changing the Block Public Access settings, ensuring a consistent security posture across the account.

356. Question #413 An ecommerce 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 emails 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?

- 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.

答案: B

解析: To reduce the time spent on resolving email delivery issues and minimize operational overhead, the solutions architect should configure the web instance to send email through Amazon Simple Email Service (Amazon SES) (Option B). Amazon SES is a scalable and cost-effective email service that is designed to send large volumes of email. By offloading the email sending responsibility to Amazon SES, the company can leverage a managed service that is optimized for email delivery, reducing the complexity and overhead associated with managing an email infrastructure.

解析: To reduce the time spent on resolving email delivery issues and minimize operational overhead, the solutions architect should configure the web instance to send email through Amazon Simple Email Service (Amazon SES) (Option B). Amazon SES is a scalable and cost-effective email service that is designed to send large volumes of email. By offloading the email sending responsibility to Amazon SES, the company can leverage a managed service that is optimized for email delivery, reducing the complexity and overhead associated with managing an email infrastructure.

357. Question #414A 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?

- 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 using SFTP.

答案: B

解析: B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway. This option requires the least administrative overhead because:
- It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.
- The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.
- All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.

解析: B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway. This option requires the least administrative overhead because:

- It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.
- The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.
- All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.

358. Question #415A 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?

- 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).

答案: A

解析: Given that the company does not know the access patterns for all the data, the most operationally efficient solution is to use S3 Intelligent-Tiering (Option A). This storage class automatically moves objects between two access tiers based on changing access patterns, eliminating the need for manual intervention and analysis of access patterns.

解析: Given that the company does not know the access patterns for all the data, the most operationally efficient solution is to use S3 Intelligent-Tiering (Option A). This storage class automatically moves objects between two access tiers based on changing access patterns, eliminating the need for manual intervention and analysis of access patterns.

359. Question #417A 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?

- 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.

答案: C

解析: The most cost-effective solution that also maintains low network latency is to purchase a Compute Savings Plan (Option C), which covers both EC2 and Lambda usage. By connecting the Lambda functions to the private subnet containing the EC2 instances, the company ensures direct network access and low latency, aligning with the application's requirements.

解析: The most cost-effective solution that also maintains low network latency is to purchase a Compute Savings Plan (Option C), which covers both EC2 and Lambda usage. By connecting the Lambda functions to the private subnet containing the EC2 instances, the company ensures direct network access and low latency, aligning with the application's requirements.

360. Question #418A 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**?

- 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.

答案: B

解析: To comply with the principle of least privilege, the solutions architect should add the development account as a principal in the trust policy of the role in the production account (Option B). This allows team

members to assume the role in the production account without granting excessive permissions, thereby maintaining security and adherence to the principle.

解析: To comply with the principle of least privilege, the solutions architect should add the development account as a principal in the trust policy of the role in the production account (Option B). This allows team members to assume the role in the production account without granting excessive permissions, thereby maintaining security and adherence to the principle.

361. Question #420 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?

- 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.

答案: D

解析: Based on the company's requirements for high availability, automatic failover, read offloading, and cost optimization, the best solution is: D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint. Here's why this solution meets the company's needs: 1. High Availability and Automatic Failover: – Multi-AZ DB cluster deployments provide high availability across multiple Availability Zones. – They offer automatic failover support, typically in less than 40 seconds, meeting the company's requirement. 2. Read

Offloading: – Multi-AZ DB clusters come with a reader endpoint that automatically load balances read traffic across available DB instances in the cluster. – This allows for efficient offloading of read queries from the primary instance.

3. Cost Optimization: – By using the reader endpoint, the company can efficiently distribute read workloads without needing to create and manage separate read replicas. – This approach is generally more cost-effective than maintaining individual read replicas.

4. Simplified Management: – The Multi-AZ DB cluster architecture simplifies database administration tasks, aligning with the company's goal to reduce time-consuming administrative work.

Best practices for implementing this solution:

1. Ensure proper monitoring and alerting are set up to track the performance and health of the DB cluster.
2. Regularly review and optimize database queries to make the most of the read offloading capabilities.
3. Implement appropriate security measures, such as encryption at rest and in transit, and use VPC security groups to control access to the DB cluster.
4. Periodically test failover scenarios to ensure the automatic failover works as expected.
5. Use AWS Identity and Access Management (IAM) to manage access to the RDS resources, following the principle of least privilege.

[1] [Amazon RDS for PostgreSQL – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_PostgreSQL.html)

[3] [Resilience in Amazon RDS – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/disaster-recovery-resiliency.html>)

[6] [Maintaining a DB instance – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)

解析: Based on the company's requirements for high availability, automatic failover, read offloading, and cost optimization, the best solution is: D. Use an Amazon RDS Multi-AZ DB cluster deployment. Point the read workload to the reader endpoint. Here's why this solution meets the company's needs:

1. High Availability and Automatic Failover: – Multi-AZ DB cluster deployments provide high availability across multiple Availability Zones. – They offer automatic failover support, typically in less than 40 seconds, meeting the company's requirement.
2. Read

Offloading: – Multi-AZ DB clusters come with a reader endpoint that automatically load balances read traffic across available DB instances in the cluster. – This allows for efficient offloading of read queries from the primary instance.

3. Cost Optimization: – By using the reader endpoint, the company can efficiently distribute read workloads without needing to create and manage separate read replicas. – This approach is generally more cost-effective than maintaining individual read replicas.

4. Simplified Management: – The Multi-AZ DB cluster architecture simplifies database administration tasks, aligning with the company's goal to reduce time-consuming administrative work.

Best practices for implementing this solution:

1. Ensure proper monitoring and alerting are set up to track the performance and health of the DB cluster.
2. Regularly review and optimize database queries to make the most of the read offloading capabilities.
3. Implement appropriate security measures, such as encryption at rest and in transit, and use VPC security groups to control access to the DB cluster.
4. Periodically test failover scenarios to ensure the automatic failover works as expected.
5. Use AWS Identity and Access Management (IAM) to manage access to the RDS resources, following the principle of least privilege.

[1] [Amazon RDS for PostgreSQL – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_PostgreSQL.html)

[3] [Resilience in Amazon RDS – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/disaster-recovery-resiliency.html>)

[6] [Maintaining a DB instance – Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)

362. Question #421A 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?

- 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.

答案：B

解析：Actually AWS Transfer Family can use S3, so it's a toss-up between Options B & C. Option B for the following reasons (based on the keys in STEM): 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. 1. Requires a serverless option that provides high IOPS performance and highly configurable security. 2. User also wants to maintain control over user permissions.

解析：Actually AWS Transfer Family can use S3, so it's a toss-up between Options B & C. Option B for the following reasons (based on the keys in

STEM) : 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.

1. Requires a serverless option that provides high IOPS performance and highly configurable security.
2. User also wants to maintain control over user permissions

363. Question #422A 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?

- 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.

答案: D

解析: Option D is the most suitable as it provides a scalable and flexible solution. By using Amazon SQS, the system can handle不规则的(irregular) workloads efficiently, as the queue will buffer incoming requests. Deploying models as Amazon ECS services allows for the use of Docker containers, which is beneficial for microservices architecture. AWS Auto Scaling can adjust the number of running container instances based on the SQS queue size, ensuring that the system can scale out to handle peak loads and scale in to save costs during periods of low activity.

解析: Option D is the most suitable as it provides a scalable and flexible solution. By using Amazon SQS, the system can handle不规则的(irregular) workloads efficiently, as the queue will buffer incoming requests. Deploying models as Amazon ECS services allows for the use of Docker containers, which is beneficial for microservices architecture. AWS Auto Scaling can adjust the number of running container instances based on the SQS queue size, ensuring that the system can scale out to handle peak loads and scale in to save costs during periods of low activity.

364. Question #424A 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?

- 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.

答案: B

解析: Option B is the most cost-effective solution. Reserved Instances for the frontend nodes ensure that these always-on instances are cost-optimized for continuous operation. Meanwhile, using Spot Instances for the backend nodes allows the company to take advantage of the lower costs associated with Spot Instances, which can be scaled out and in based on demand without incurring the higher costs of On-Demand Instances or Reserved Instances.

解析: Option B is the most cost-effective solution. Reserved Instances for the frontend nodes ensure that these always-on instances are cost-optimized for continuous operation. Meanwhile, using Spot Instances for the backend nodes allows the company to take advantage of the lower costs associated with Spot Instances, which can be scaled out and in based on demand without incurring the higher costs of On-Demand Instances or Reserved Instances.

365. Question #425A company uses high block storage capacity to runs 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?

- A. GP2 volume type
- B. io2 volume type
- C. GP3 volume type
- D. io1 volume type

答案: C

解析: Option C, the GP3 volume type, is the most cost-effective solution for the given requirements. GP3 volumes provide a balance of performance and cost, allowing for up to 16,000 IOPS, which exceeds the company's peak requirement of 15,000 IOPS. They also offer the ability to scale performance independently of capacity, which aligns with the company's

needs.

解析: Option C, the GP3 volume type, is the most cost-effective solution for the given requirements. GP3 volumes provide a balance of performance and cost, allowing for up to 16,000 IOPS, which exceeds the company's peak requirement of 15,000 IOPS. They also offer the ability to scale performance independently of capacity, which aligns with the company's needs.

366. Question #426A 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?

- 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.

答案: A

解析: Option A is the correct choice because AWS DataSync is designed for securely and efficiently transferring large amounts of data to AWS, including Amazon S3. It can help the company to migrate its healthcare application data with minimal downtime. Additionally, AWS CloudTrail can log data events, which is essential for providing audit access at all levels as required by the new regulation.

解析: Option A is the correct choice because AWS DataSync is designed for securely and efficiently transferring large amounts of data to AWS, including Amazon S3. It can help the company to migrate its healthcare application data with minimal downtime. Additionally, AWS CloudTrail can

log data events, which is essential for providing audit access at all levels as required by the new regulation.

367. Question #427A 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?

- 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.

答案：B

解析：Option B is the appropriate solution because **AWS Elastic Beanstalk is designed to deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications.** It supports Java applications and can be configured to run on Apache Tomcat, which meets the requirements for the Java application deployment.

Additionally, Elastic Beanstalk can be set up with a load-balanced environment and a rolling deployment policy to ensure high availability.

解析：Option B is the appropriate solution because **AWS Elastic Beanstalk is designed to deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications.** It supports Java applications and can be configured to run on Apache Tomcat, which meets the requirements for the Java application deployment.

Additionally, Elastic Beanstalk can be set up with a load-balanced environment and a rolling deployment policy to ensure high availability.

368. Question #428A 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?**

- 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.

答案：B

解析：Option B is the most secure approach as it involves creating an IAM role with the necessary permissions and attaching that role to the Lambda function. This method adheres to the principle of least privilege and does not require storing access keys within the Lambda environment or code, reducing the risk of key exposure.

解析：Option B is the most secure approach as it involves creating an IAM role with the necessary permissions and attaching that role to the Lambda function. This method adheres to the principle of least privilege and does not require storing access keys within the Lambda environment or code, reducing the risk of key exposure.

369. Question #429The 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}  
            }  
        }  
    ]  
}
```

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region.
- 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.

答案：D

解析：The correct answer is D. According to AWS IAM policy evaluation logic, when a permission statement is followed by a condition (like requiring MFA), only the specific actions listed are allowed with that condition. In this case, only the actions ec2:StopInstances and ec2:TerminateInstances are allowed with MFA in the us-east-1 Region. Other EC2 actions are allowed without conditions in the same region.

解析：The correct answer is D. According to AWS IAM policy evaluation logic, when a permission statement is followed by a condition (like requiring MFA), only the specific actions listed are allowed with that condition. In this case, only the actions ec2:StopInstances and ec2:TerminateInstances are allowed with MFA in the us-east-1 Region. Other EC2 actions are allowed without conditions in the same region.

370. Question #431A 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?

- 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.

答案：B

解析: Option B is the correct choice because Amazon ElastiCache for Redis is a versatile, in-memory data store that can be used to store and rank scores in real time. Redis supports data structures like sorted sets, which are ideal for leaderboards. By using Redis, the system can quickly update and retrieve the top scores, ensuring near real-time scoreboard updates.

解析: Option B is the correct choice because Amazon ElastiCache for Redis is a versatile, in-memory data store that can be used to store and rank scores in real time. Redis supports data structures like sorted sets, which are ideal for leaderboards. By using Redis, the system can quickly update and retrieve the top scores, ensuring near real-time scoreboard updates.

371. Question #432 An ecommerce 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?

- 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.

答案: B

解析: Option B is the most straightforward solution with the least operational overhead. Amazon SageMaker is a fully managed service that enables developers and data scientists to build, train, and deploy ML models quickly and efficiently. Amazon QuickSight, on the other hand, is

a business analytics service that can be used to create visualizations, reports, and dashboards. It can easily integrate with SageMaker to visualize the data processed by the ML models.

解析: Option B is the most straightforward solution with the least operational overhead. Amazon SageMaker is a fully managed service that enables developers and data scientists to build, train, and deploy ML models quickly and efficiently. Amazon QuickSight, on the other hand, is a business analytics service that can be used to create visualizations, reports, and dashboards. It can easily integrate with SageMaker to visualize the data processed by the ML models.

372. Question #433A 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?

- 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.

答案: C

解析: Option C is the correct solution. A service control policy (SCP) in AWS Organizations allows you to define the maximum permissions that users and roles in member accounts can have. By creating an SCP that prevents tag modification, you can enforce governance over the tags used for cost tracking across multiple accounts, ensuring that only authorized changes can be made.

解析: Option C is the correct solution. A service control policy (SCP) in AWS Organizations allows you to define the maximum permissions that users and roles in member accounts can have. By creating an SCP that prevents tag modification, you can enforce governance over the tags used for cost tracking across multiple accounts, ensuring that only authorized changes

can be made.

373. Question #434A 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?

- 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.

答案：A

解析：Option A is the solution that would result in the least amount of downtime. By configuring the DynamoDB table as a global table, the data is replicated across multiple regions, including the new disaster recovery region. This setup allows for a seamless switchover with minimal impact on availability. Additionally, DNS failover can be used to redirect traffic to the new region without the need for manual intervention, which further reduces downtime.

解析：Option A is the solution that would result in the least amount of downtime. By configuring the DynamoDB table as a global table, the data is replicated across multiple regions, including the new disaster

recovery region. This setup allows for a seamless switchover with minimal impact on availability. Additionally, DNS failover can be used to redirect traffic to the new region without the need for manual intervention, which further reduces downtime.

374. Question #435A 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**?

- 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.

答案: A

解析: Option A is the most cost-effective solution for migrating a large database like the one described. AWS Snowball Edge Storage Optimized is designed for petabyte-scale data transfers both on-premises and off-premises. Using AWS DMS with AWS SCT allows for ongoing database changes to be replicated, ensuring minimal downtime. The use of a 1 GB AWS Direct Connect (Option D) might be expensive and not necessarily

faster than using Snowball Edge for a 20 TB database.

解析: Option A is the most cost-effective solution for migrating a large database like the one described. AWS Snowball Edge Storage Optimized is designed for petabyte-scale data transfers both on-premises and off-premises. Using AWS DMS with AWS SCT allows for ongoing database changes to be replicated, ensuring minimal downtime. The use of a 1 GB AWS Direct Connect (Option D) might be expensive and not necessarily faster than using Snowball Edge for a 20 TB database.

375. Question #436A 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?**

- 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.

答案: A

解析: Option A is the most cost-effective solution as it allows the company to increase the size of the existing RDS instance to handle the increased workload. Reserved instances can offer significant cost savings over on-demand instances, especially for a workload that is expected to be consistent. Upgrading the instance size will provide the necessary resources without the need to add additional infrastructure.

解析: Option A is the most cost-effective solution as it allows the company to increase the size of the existing RDS instance to handle the increased workload. Reserved instances can offer significant cost savings over on-demand instances, especially for a workload that is expected to be consistent. Upgrading the instance size will provide the necessary

resources without the need to add additional infrastructure.

376. Question #437A 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?

- 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.

答案: B

解析: Option B is the recommended solution. AWS WAF (Web Application Firewall) can be used to create custom rules to block illegitimate traffic while allowing legitimate users to access the website. By associating WAF with the ALB, the company can implement rate-based rules to limit the number of requests from a given IP address, which can help mitigate DDoS attacks without impacting legitimate traffic.

解析: Option B is the recommended solution. AWS WAF (Web Application Firewall) can be used to create custom rules to block illegitimate traffic while allowing legitimate users to access the website. By associating WAF with the ALB, the company can implement rate-based rules to limit the number of requests from a given IP address, which can help mitigate DDoS attacks without impacting legitimate traffic.

377. Question #438A 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?

- 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.**

答案: D

解析: Option D is the most secure method for sharing the database with an external auditor. By creating an encrypted snapshot and sharing it, the company ensures that the data is protected both in transit and at rest. Additionally, granting the auditor access to the AWS KMS encryption key allows them to decrypt and access the data while maintaining control over the encryption keys.

解析: Option D is the most secure method for sharing the database with an external auditor. By creating an encrypted snapshot and sharing it, the company ensures that the data is protected both in transit and at rest. Additionally, granting the auditor access to the AWS KMS encryption key allows them to decrypt and access the data while maintaining control over the encryption keys.

378. Question #439A 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**?

- 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. 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.

答案：A

解析：Option A is the solution that requires the least operational overhead. By expanding the VPC with an additional IPv4 CIDR block, the architect can increase the available IP addresses without the need to set up complex networking solutions like VPC peering or VPN connections. This approach simplifies network management and reduces the operational burden.

解析：Option A is the solution that requires the least operational overhead. By expanding the VPC with an additional IPv4 CIDR block, the architect can increase the available IP addresses without the need to set up complex networking solutions like VPC peering or VPN connections. This approach simplifies network management and reduces the operational burden.

379. Question #441A 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?

- 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.

答案: C

解析: Option C is the most cost-effective solution for serving static web content. Amazon CloudFront is a content delivery network (CDN) that can cache and deliver static content from an S3 bucket, reducing the load on the EC2 instances. This can lead to a decrease in the number of required On-Demand Instances, thereby optimizing costs.

解析: Option C is the most cost-effective solution for serving static web content. Amazon CloudFront is a content delivery network (CDN) that can cache and deliver static content from an S3 bucket, reducing the load on the EC2 instances. This can lead to a decrease in the number of required On-Demand Instances, thereby optimizing costs.

380. Question #442A 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?

- 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.

答案：D

解析：Option D is the most efficient solution as it allows for fine-grained access control using tags. Lake Formation can manage permissions across multiple accounts, and by using tag-based access control, the company can ensure that only the engineering team has access to the necessary data. This approach requires less operational overhead compared to manually copying data or setting up individual permissions.

解析：Option D is the most efficient solution as it allows for fine-grained access control using tags. Lake Formation can manage permissions across multiple accounts, and by using tag-based access control, the company can ensure that only the engineering team has access to the necessary data. This approach requires less operational overhead compared to manually copying data or setting up individual permissions.

381. Question #443A 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?

- 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.

答案：A

解析：Option A is the most suitable for the requirements. Amazon S3 with Transfer Acceleration can significantly reduce the time it takes to upload and download large files globally. It does this by leveraging

Amazon CloudFront's globally distributed edge locations to create an optimized route for the data transfer. This results in lower latency and higher transfer speeds, which is ideal for users distributed across different geographic regions.

解析: Option A is the most suitable for the requirements. Amazon S3 with Transfer Acceleration can significantly reduce the time it takes to upload and download large files globally. It does this by leveraging Amazon CloudFront's globally distributed edge locations to create an optimized route for the data transfer. This results in lower latency and higher transfer speeds, which is ideal for users distributed across different geographic regions.

382. Question #444A 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?

- 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.

答案: B

解析: Option B is the best approach to maximize reliability. By making the RDS instance Multi-AZ, the database is protected against zone failures. Enabling deletion protection prevents accidental termination of the DB instance. Placing the EC2 instances behind an Application Load Balancer and using an Auto Scaling group across multiple Availability Zones ensures that the web servers remain available even if there is a failure in one zone. This setup provides both high availability and fault tolerance.

解析: Option B is the best approach to maximize reliability. By making the RDS instance Multi-AZ, the database is protected against zone failures. Enabling deletion protection prevents accidental termination of the DB instance. Placing the EC2 instances behind an Application Load Balancer and using an Auto Scaling group across multiple Availability Zones ensures that the web servers remain available even if there is a failure in one zone. This setup provides both high availability and fault tolerance.

383. Question #445A 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?

- 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.

答案: A

解析: Option A is the most efficient and meets the requirement of not disrupting access and updates to the data during the transfer window. AWS DataSync can automate the transfer of data to Amazon S3 and is designed to work with AWS Direct Connect for fast and secure data transfer. This solution allows the company to maintain access to the data during the transfer process, which is not possible with the shipping options B and D.

解析: Option A is the most efficient and meets the requirement of not disrupting access and updates to the data during the transfer window. AWS DataSync can automate the transfer of data to Amazon S3 and is designed to work with AWS Direct Connect for fast and secure data transfer. This solution allows the company to maintain access to the data during the transfer process, which is not possible with the shipping options B and D.

384. Question #446A 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?

- 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.

答案：D

解析：Option D is the most efficient solution as it uses S3 Batch Operations to apply Object Lock with compliance retention to existing data. This method does not require recopying all existing objects, which would be resource-intensive and time-consuming. Compliance retention mode ensures that the data cannot be deleted or overwritten for the duration of the retention period, meeting the legal requirement.

解析：Option D is the most efficient solution as it uses S3 Batch Operations to apply Object Lock with compliance retention to existing data. This method does not require recopying all existing objects, which would be resource-intensive and time-consuming. Compliance retention mode ensures that the data cannot be deleted or overwritten for the duration of the retention period, meeting the legal requirement.

385. Question #447A 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?

- 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.

答案：A

解析: To deploy the stateless web application across multiple AWS Regions and provide Regional failover capabilities, the best solution is: A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration. Here's how to implement this solution and why it's the most effective approach:

1. Deploy the application in multiple Regions:
 - Set up Lambda functions and API Gateway in each desired Region.
 - Ensure the application code and configurations are consistent across Regions.
2. Create Route 53 health checks:
 - In the Route 53 console, create a health check for each Region's API Gateway endpoint.
 - Configure appropriate thresholds and intervals for the health checks.
3. Set up Route 53 DNS records:
 - Create a Route 53 record set for your application's domain.
 - Configure it as an active-active failover using the API Gateway endpoints from each Region.
 - Associate the corresponding health checks with each endpoint.
4. Implement active-active failover:
 - Route 53 will distribute traffic across healthy endpoints.
 - If a Region becomes unhealthy, Route 53 will automatically route traffic to the healthy Region(s).
 - This solution is optimal because:
 - It provides true multi-Region failover with minimal latency.
 - It allows for easy scaling by adding more Regions as needed.
 - Route 53's global network of DNS servers ensures low-latency responses worldwide.
 - The active-active configuration improves overall application availability and performance.
 - It's cost-effective, as you only pay for the Route 53 health checks and DNS queries.

Best practices to consider:

1. Use infrastructure as code (e.g., AWS CloudFormation) to maintain consistency across Regions.
2. Implement proper monitoring and alerting for your multi-Region deployment.
3. Regularly test your failover mechanism to ensure it works as expected.
4. Consider using AWS Global Accelerator for additional performance benefits and simplified global routing.

REF: [1] [Amazon API Gateway concepts – Amazon API Gateway] (<https://docs.aws.amazon.com/api-gateway/latest/developerguide/api-gateway-basic-concept.html>) [3]

[REL10-BP01 Deploy the workload to multiple locations – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/latest/framework/rel_fault_isolation_multiaz_region_system.html) [6]

[Deploy a reference architecture that models a serverless active/passive workload with asynchronous replication of application data and failover from a primary to a secondary AWS Region – Multi-Region Application Architecture Solution] (<https://docs.aws.amazon.com/solutions/latest/multi-region-application-architecture/welcome.html>)

解析：To deploy the stateless web application across multiple AWS Regions and provide Regional failover capabilities, the best solution is: A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration. Here's how to implement this solution and why it's the most effective approach:

1. Deploy the application in multiple Regions:
 - Set up Lambda functions and API Gateway in each desired Region.
 - Ensure the application code and configurations are consistent across Regions.
2. Create Route 53 health checks:
 - In the Route 53 console, create a health check for each Region's API Gateway endpoint.
 - Configure appropriate thresholds and intervals for the health checks.
3. Set up Route 53 DNS records:
 - Create a Route 53 record set for your application's domain.
 - Configure it as an active-active failover using the API Gateway endpoints from each Region.
 - Associate the corresponding health checks with each endpoint.
4. Implement active-active failover:
 - Route 53 will distribute traffic across healthy endpoints.
 - If a Region becomes unhealthy, Route 53 will automatically route traffic to the healthy Region(s).
 - This solution is optimal because:
 - It provides true multi-Region failover with minimal latency.
 - It allows for easy scaling by adding more Regions as needed.
 - Route 53's global network of DNS servers ensures low-latency responses worldwide.
 - The active-active configuration improves overall application availability and performance.
 - It's cost-effective, as you only pay for the Route 53 health checks and DNS queries.

Best practices to consider:

1. Use infrastructure as code (e.g., AWS CloudFormation) to maintain consistency across Regions.
2. Implement proper monitoring and alerting for your multi-Region deployment.
3. Regularly test your failover mechanism to ensure it works as expected.
4. Consider using AWS Global Accelerator for additional performance benefits and simplified global routing.

REF: [1] [Amazon API

Gateway concepts – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-basic-concept.html>) [3]

[REL10-BP01 Deploy the workload to multiple locations – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/latest/framework/rel_fault_isolation_multiaz_region_system.html) [6]

[Deploy a reference architecture that models a serverless active/passive workload with asynchronous replication of application data and failover from a primary to a secondary AWS Region – Multi-Region Application Architecture Solution] (<https://docs.aws.amazon.com/solutions/latest/multi-region-application-architecture/welcome.html>)

386. Question #448A 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?

- 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.

答案: C

解析: Option C is the solution that mitigates the single point of failure. By adding a second set of VPNs from a second customer gateway device, the Management VPC gains an additional path for connectivity, ensuring that if one VPN connection fails, the other can still be used.

解析: Option C is the solution that mitigates the single point of failure. By adding a second set of VPNs from a second customer gateway device, the Management VPC gains an additional path for connectivity,

ensuring that if one VPN connection fails, the other can still be used.

387. Question #449A 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**?

- 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.

答案: B

解析: Option B is the most cost-effective solution as it allows the company to use Amazon RDS Custom for Oracle, which supports customization of the database engine to accommodate third-party features that require privileged access. This option is more cost-effective than migrating to an EC2 instance (Option C), which would require more management and maintenance, or rewriting the application code (Option D).

解析: Option B is the most cost-effective solution as it allows the company to use Amazon RDS Custom for Oracle, which supports customization of the database engine to accommodate third-party features that require privileged access. This option is more cost-effective than migrating to an EC2 instance (Option C), which would require more management and maintenance, or rewriting the application code (Option D).

388. Question #452A 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?

- 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.

答案：B

解析：Option B is the most cost-effective solution. AWS Lambda allows you to run code without provisioning or managing servers, and it scales automatically with the number of requests. Since the job is short-running and occurs on an hourly schedule, Lambda is a suitable choice as it charges based on the number of requests and the time the code executes.

解析：Option B is the most cost-effective solution. AWS Lambda allows you to run code without provisioning or managing servers, and it scales automatically with the number of requests. Since the job is short-running and occurs on an hourly schedule, Lambda is a suitable choice as it charges based on the number of requests and the time the code executes.

389. Question #453A 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?

- 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.

答案: D

解析: Option D is the correct solution. AWS Backup with a vault lock in compliance mode ensures that backups cannot be modified or deleted for the duration of the retention period, which aligns with the regulatory requirements. The vault lock feature provides an additional layer of protection to prevent accidental or unauthorized changes to the backup plans.

解析: Option D is the correct solution. AWS Backup with a vault lock in compliance mode ensures that backups cannot be modified or deleted for the duration of the retention period, which aligns with the regulatory requirements. The vault lock feature provides an additional layer of protection to prevent accidental or unauthorized changes to the backup plans.

390. Question #454A 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**?

- 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.

答案: C

解析: Option C is the most operationally efficient solution. Workload Discovery on AWS is designed to automatically discover and map the relationships between resources across multiple accounts and Regions. This service can help the solutions architect quickly understand the resource inventory and relationships without the need for manual processes or additional tooling.

解析: Option C is the most operationally efficient solution. Workload Discovery on AWS is designed to automatically discover and map the relationships between resources across multiple accounts and Regions. This service can help the solutions architect quickly understand the resource inventory and relationships without the need for manual processes or additional tooling.

391. Question #456A 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?

- 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.

答案: C

解析: Option C is the most cost-effective solution as it leverages AWS Backup, which is a fully managed service that can automate and streamline the process of creating backups across Regions. Configuring cross-Region backup ensures that EC2 instances are backed up to a second Region

without the need to manually manage the replication of data.

解析: Option C is the most cost-effective solution as it leverages AWS Backup, which is a fully managed service that can automate and streamline the process of creating backups across Regions. Configuring cross-Region backup ensures that EC2 instances are backed up to a second Region without the need to manually manage the replication of data.

392. Question #457A 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?

- 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.

答案: C

解析: Option C is the correct solution. AWS Transfer Family supports the AS2 protocol, which is required for secure data transfer. Additionally, AWS Lambda can be used to create custom authentication mechanisms, including integrating with the company's existing IdP for user authentication.

解析: Option C is the correct solution. AWS Transfer Family supports the AS2 protocol, which is required for secure data transfer. Additionally, AWS Lambda can be used to create custom authentication mechanisms, including integrating with the company's existing IdP for user authentication.

393. Question #459A 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?

- 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.

答案：A

解析：Option A is the most operationally efficient solution. By activating a user-defined cost allocation tag named "department" at the management account level, the accounting team can ensure that this tag is consistently applied across all member accounts. Then, using Cost Explorer, they can create a cost report that groups and filters by this tag, allowing them to allocate EC2 costs by department.

解析：Option A is the most operationally efficient solution. By activating a user-defined cost allocation tag named "department" at the management account level, the accounting team can ensure that this tag is consistently applied across all member accounts. Then, using Cost Explorer, they can create a cost report that groups and filters by this tag, allowing them to allocate EC2 costs by department.

394. Question #460A company wants to securely exchange data between its software as a service (SaaS) 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 method should the solutions architect select?

- 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.

答案：C

解析：Option C is the correct choice. Amazon AppFlow is a fully managed service that can securely transfer data between Salesforce and Amazon S3. It supports encryption in transit and allows the use of AWS KMS CMKs for encrypting data at rest, meeting the company's security requirements.

解析：Option C is the correct choice. Amazon AppFlow is a fully managed service that can securely transfer data between Salesforce and Amazon S3. It supports encryption in transit and allows the use of AWS KMS CMKs for encrypting data at rest, meeting the company's security requirements.

395. Question #461A 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?

- 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.

答案：B

解析：Option B is the correct solution. AWS Global Accelerator can improve the availability and performance of applications for global users. By creating an NLB behind a Global Accelerator endpoint, the company can ensure that traffic is distributed to the optimal EC2 instances in the Auto Scaling group, reducing latency for gaming app users.

解析：Option B is the correct solution. AWS Global Accelerator can improve the availability and performance of applications for global users. By creating an NLB behind a Global Accelerator endpoint, the company can ensure that traffic is distributed to the optimal EC2 instances in the Auto Scaling group, reducing latency for gaming app users.

396. Question #462A 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?

- 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.

答案：B

解析：Option B is the correct approach. By using Amazon SQS, the system can decouple the order processing from the order ingestion. Orders are written to the SQS queue, which acts as a buffer during high-traffic periods. EC2 instances in an Auto Scaling group can then process the orders from the queue, ensuring that no orders are lost and the system can handle the workload efficiently.

解析：Option B is the correct approach. By using Amazon SQS, the system can decouple the order processing from the order ingestion. Orders are written to the SQS queue, which acts as a buffer during high-traffic periods. EC2 instances in an Auto Scaling group can then process the orders from the queue, ensuring that no orders are lost and the system can handle the workload efficiently.

397. Question #463An 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?

- 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

答案: C

解析: Option C is the most cost-effective solution. AWS Lambda allows for running code in response to triggers, such as the arrival of new data in an S3 bucket. Given the small amount of data (2 MB) and the short processing time required, Lambda can execute the necessary Python script to process the data and produce the summary results efficiently.

解析: Option C is the most cost-effective solution. AWS Lambda allows for running code in response to triggers, such as the arrival of new data in an S3 bucket. Given the small amount of data (2 MB) and the short processing time required, Lambda can execute the necessary Python script to process the data and produce the summary results efficiently.

398. Question #464A 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?

- 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.

答案：A

解析：Option A is the correct solution. Converting the PostgreSQL database to a Multi-AZ deployment in Amazon RDS will automatically create a synchronous standby replica in a different Availability Zone. This setup provides data redundancy, eliminates the single point of failure, and maintains the database's availability without any application code changes.

解析：Option A is the correct solution. Converting the PostgreSQL database to a Multi-AZ deployment in Amazon RDS will automatically create a synchronous standby replica in a different Availability Zone. This setup provides data redundancy, eliminates the single point of failure, and maintains the database's availability without any application code changes.

399. Question #465A 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?

- 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

答案：C

解析：Option C is the correct choice. Amazon EBS Multi-Attach feature allows a single EBS volume to be attached to multiple EC2 instances in the same Availability Zone. The io2 volume type is designed to deliver

high and consistent performance, making it suitable for I/O-intensive workloads that require the ability to write to multiple volumes simultaneously.

解析: Option C is the correct choice. Amazon EBS Multi-Attach feature allows a single EBS volume to be attached to multiple EC2 instances in the same Availability Zone. The io2 volume type is designed to deliver high and consistent performance, making it suitable for I/O-intensive workloads that require the ability to write to multiple volumes simultaneously.

400. Question #466A 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?

- 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

答案: A

解析: Option A is the correct solution. By configuring the EC2 instances to be part of an Auto Scaling group and enabling Multi-AZ for the RDS instance, the application can achieve high availability. Additionally, an Application Load Balancer can distribute traffic across the EC2 instances, further enhancing availability and fault tolerance.

解析: Option A is the correct solution. By configuring the EC2 instances to be part of an Auto Scaling group and enabling Multi-AZ for the RDS instance, the application can achieve high availability. Additionally, an Application Load Balancer can distribute traffic across the EC2 instances, further enhancing availability and fault tolerance.

401. Question #467A 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?

- 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.

答案：B

解析：Option B is the correct action. By enabling discount sharing in the management account, the company can share the unused compute savings with other accounts within the organization, ensuring that the commitment is fully utilized and the company receives the maximum benefit from the Compute Savings Plan.

解析：Option B is the correct action. By enabling discount sharing in the management account, the company can share the unused compute savings with other accounts within the organization, ensuring that the commitment is fully utilized and the company receives the maximum benefit from the Compute Savings Plan.

402. Question #468A 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?

- 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.

答案：B

解析：Option B is the correct solution. Amazon API Gateway can be used to create a REST API that serves as the frontend interface for the microservices application. By hosting the application in Amazon ECS within a private subnet and setting up a private VPC link, the API Gateway can securely access the backend services without exposing them to the public internet.

解析：Option B is the correct solution. Amazon API Gateway can be used to create a REST API that serves as the frontend interface for the microservices application. By hosting the application in Amazon ECS within a private subnet and setting up a private VPC link, the API Gateway can securely access the backend services without exposing them to the public internet.

403. Question #469A 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?

- 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

答案: C

解析: Option C is the correct solution. S3 Intelligent-Tiering automatically moves objects between access tiers based on access patterns, which is suitable for data with unpredictable access patterns. This feature can help reduce storage costs by moving infrequently accessed data to lower-cost storage tiers.

解析: Option C is the correct solution. S3 Intelligent-Tiering automatically moves objects between access tiers based on access patterns, which is suitable for data with unpredictable access patterns. This feature can help reduce storage costs by moving infrequently accessed data to lower-cost storage tiers.

404. Question #470A 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?

- 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

答案: D

解析: Option D is the correct solution. An egress-only internet gateway allows IPv6 traffic to be routed from the VPC to the internet for outbound (egress) traffic only. This setup ensures that the EC2 instances can initiate connections to external services while preventing any inbound connections, adhering to the company's security policy.

解析: Option D is the correct solution. An egress-only internet gateway allows IPv6 traffic to be routed from the VPC to the internet for outbound (egress) traffic only. This setup ensures that the EC2 instances can initiate connections to external services while preventing any inbound connections, adhering to the company's security policy.

405. Question #471A 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?

- 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

答案: C

解析: Option C is the correct solution. A gateway VPC endpoint for Amazon S3 allows for private connectivity between the VPC and S3, ensuring that data transfer between the application running in the VPC and the S3 bucket stays within the AWS network. This prevents traffic from traversing the public internet, reducing costs and enhancing security.

解析: Option C is the correct solution. A gateway VPC endpoint for Amazon S3 allows for private connectivity between the VPC and S3, ensuring that data transfer between the application running in the VPC and the S3 bucket stays within the AWS network. This prevents traffic from traversing the public internet, reducing costs and enhancing security.

406. Question #472A 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?

- 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.

答案：A

解析：Option A is the correct solution. DAX is a fully managed, high-performance in-memory caching service for DynamoDB that can significantly reduce the latency of read operations. By configuring DAX for the new messages table and updating the application to use the DAX endpoint, the architect can achieve low-latency access to new messages with minimal application changes.

解析：Option A is the correct solution. DAX is a fully managed, high-performance in-memory caching service for DynamoDB that can significantly reduce the latency of read operations. By configuring DAX for the new messages table and updating the application to use the DAX endpoint, the architect can achieve low-latency access to new messages with minimal application changes.

407. Question #473A 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 the company do?

- 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

答案：A

解析：Option A is the correct solution. Amazon CloudFront is a content delivery network (CDN) service that can cache static content from the website at edge locations worldwide. By doing so, it reduces the load on the EC2 instances and can significantly decrease the cost by offloading traffic and reducing data transfer.

解析：Option A is the correct solution. Amazon CloudFront is a content delivery network (CDN) service that can cache static content from the website at edge locations worldwide. By doing so, it reduces the load on the EC2 instances and can significantly decrease the cost by offloading traffic and reducing data transfer.

408. Question #474A 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?

- 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.

答案：C

解析：Based on the company's requirement to enable communication between multiple VPCs across all AWS Regions with the least administrative effort, the best solution is: C. **Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.** Here's why this is the most suitable option:

1. Scalability: AWS Transit Gateway acts as a central hub, simplifying network architecture and reducing the number of connections needed between VPCs.
2. Cross-Region Support: Transit Gateway peering allows for seamless communication between VPCs in different Regions, meeting the company's requirement for inter-Region connectivity.
3. Ease of Management: Compared to other options, Transit Gateway provides a more centralized and easier-to-manage approach for connecting multiple VPCs across Regions.
4. Transitive Routing: Transit Gateway supports transitive routing, allowing all connected VPCs to communicate with each other without the need for individual peering connections.
5. Reduced Administrative Effort: Once set up, Transit Gateway requires less ongoing management compared to maintaining multiple individual VPC peering connections or other solutions.
6. Future Scalability: As the company grows and adds more VPCs or Regions, the Transit Gateway architecture can easily accommodate these changes without significant reconfiguration.
7. Integration with Other Services: Transit Gateway can integrate with other AWS networking services, providing flexibility for future network design changes.

While implementing this solution, consider the following best practices:

- Use resource sharing through AWS Resource Access Manager (RAM) to share Transit Gateways across accounts if needed.
- Implement proper route table management to control traffic flow between VPCs.
- Use Network Access Control Lists (NACLs) and Security Groups to enforce security at the VPC and instance level.
- Monitor network traffic using AWS CloudWatch and VPC Flow Logs for security and performance optimization.
- Regularly review and update your network architecture to ensure it meets evolving business needs and security requirements.

REF:
[1] [Communicating across VPCs and AWS Regions – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/secur>

e-outbound-network-traffic/vpc-region-communication.html) [3] [Community | Multi-Region Networking on AWS] (<https://community.aws/content/2eSxvGCQ02hK5z8GseirTsE7BV4/multi-region-networking-on-aws>) [6] [VPC to VPC connectivity – Building a Scalable and Secure Multi-VPC AWS Network Infrastructure] (<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html>)

解析: Based on the company's requirement to enable communication between multiple VPCs across all AWS Regions with the least administrative effort, the best solution is: C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications. Here's why this is the most suitable option:

1. **Scalability:** AWS Transit Gateway acts as a central hub, simplifying network architecture and reducing the number of connections needed between VPCs.
2. **Cross-Region Support:** Transit Gateway peering allows for seamless communication between VPCs in different Regions, meeting the company's requirement for inter-Region connectivity.
3. **Ease of Management:** Compared to other options, Transit Gateway provides a more centralized and easier-to-manage approach for connecting multiple VPCs across Regions.
4. **Transitive Routing:** Transit Gateway supports transitive routing, allowing all connected VPCs to communicate with each other without the need for individual peering connections.
5. **Reduced Administrative Effort:** Once set up, Transit Gateway requires less ongoing management compared to maintaining multiple individual VPC peering connections or other solutions.
6. **Future Scalability:** As the company grows and adds more VPCs or Regions, the Transit Gateway architecture can easily accommodate these changes without significant reconfiguration.
7. **Integration with Other Services:** Transit Gateway can integrate with other AWS networking services, providing flexibility for future network design changes.

While implementing this solution, consider the following best practices:

- Use resource sharing through AWS Resource Access Manager (RAM) to share Transit Gateways across accounts if needed.
- Implement proper route table management to control traffic flow between VPCs.
- Use Network Access Control Lists (NACLs) and Security Groups to

enforce security at the VPC and instance level. – Monitor network traffic using AWS CloudWatch and VPC Flow Logs for security and performance optimization. – Regularly review and update your network architecture to ensure it meets evolving business needs and security requirements. REF: [1] [Communicating across VPCs and AWS Regions – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/security-outbound-network-traffic/vpc-region-communication.html>) [3] [Community | Multi-Region Networking on AWS] (<https://community.aws/content/2eSxvGCQ02hK5z8GseirTsE7BV4/multi-region-networking-on-aws>) [6] [VPC to VPC connectivity – Building a Scalable and Secure Multi-VPC AWS Network Infrastructure] (<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html>)

409. Question #475A 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?

- 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

答案: C

解析: Option C is the correct solution. Amazon EFS provides a scalable and highly durable file system that can be accessed by multiple EC2 instances in a VPC. It can be mounted in each Availability Zone, and its data can be backed up and replicated to another Region using AWS Backup, which supports backing up EFS file systems across Regions.

解析: Option C is the correct solution. Amazon EFS provides a scalable and highly durable file system that can be accessed by multiple EC2 instances in a VPC. It can be mounted in each Availability Zone, and its data can be backed up and replicated to another Region using AWS Backup, which supports backing up EFS file systems across Regions.

410. Question #476A 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?

- 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

答案: C

解析: Option C is the most secure approach. By creating an IAM policy that specifies the least privilege permissions and attaching this policy to the IAM groups, the architect ensures that all users in those groups receive only the necessary permissions. This adheres to the principle of least privilege, which is a best practice for secure access management.

解析: Option C is the most secure approach. By creating an IAM policy that specifies the least privilege permissions and attaching this policy to the IAM groups, the architect ensures that all users in those groups receive only the necessary permissions. This adheres to the principle of least privilege, which is a best practice for secure access management.

411. Question #478A 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**?

- 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.

答案：B

解析：Option B is the most secure solution. By enabling S3 Versioning, the law firm can keep a complete version history of the objects in the bucket, which helps protect against accidental deletions. S3 Object Lock with a retention period ensures that the files cannot be modified or deleted before the designated date. Configuring the bucket for static website hosting allows public access to the files, and an S3 bucket policy can be set to enforce read-only access.

解析：Option B is the most secure solution. By enabling S3 Versioning, the law firm can keep a complete version history of the objects in the bucket, which helps protect against accidental deletions. S3 Object Lock with a retention period ensures that the files cannot be modified or deleted before the designated date. Configuring the bucket for static website hosting allows public access to the files, and an S3 bucket policy can be set to enforce read-only access.

412. Question #479A 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?

- 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.

答案：B

解析：Option B is the recommended solution. AWS CloudFormation allows the infrastructure to be defined as a template and can automate the deployment of the entire stack, which includes resources like an Auto Scaling group, an Application Load Balancer, and an Amazon RDS database. This approach ensures that the infrastructure can be consistently and repeatedly deployed across different environments and Availability Zones.

解析：Option B is the recommended solution. AWS CloudFormation allows the infrastructure to be defined as a template and can automate the deployment of the entire stack, which includes resources like an Auto Scaling group, an Application Load Balancer, and an Amazon RDS database. This approach ensures that the infrastructure can be consistently and repeatedly deployed across different environments and Availability Zones.

413. Question #480A 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?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint**
- C. Private subnet
- D. Virtual private gateway

答案：B

解析：Option B, VPC endpoint, is the correct choice. A VPC endpoint for Amazon S3 enables private connections between your VPC and Amazon S3, ensuring that traffic between the EC2 instances and S3 does not leave the AWS network and does not traverse the public internet.

解析：Option B, VPC endpoint, is the correct choice. A VPC endpoint for Amazon S3 enables private connections between your VPC and Amazon S3, ensuring that traffic between the EC2 instances and S3 does not leave the AWS network and does not traverse the public internet.

414. Question #481A 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?

- 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

答案：B

解析：Option B, the write-through caching strategy, is the correct solution. This strategy ensures that any data added to or updated in the database is immediately reflected in the cache, maintaining data consistency between the cache and the database.

解析: Option B, the write-through caching strategy, is the correct solution. This strategy ensures that any data added to or updated in the database is immediately reflected in the cache, maintaining data consistency between the cache and the database.

415. Question #482A 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**?

- 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

答案: B

解析: Option B, using **AWS DataSync**, is the solution that will meet the requirements with the least operational overhead. DataSync is designed to automate the transfer of data between on-premises storage and AWS services like S3, and it supports encryption of data in transit.

解析: Option B, using AWS DataSync, is the solution that will meet the requirements with the least operational overhead. DataSync is designed to automate the transfer of data between on-premises storage and AWS services like S3, and it supports encryption of data in transit.

416. Question #483A 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**?

- 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.

答案：B

解析：Option B, using AWS Batch with AWS Fargate, is the most cost-effective solution. AWS Batch manages the job scheduling and executes the job in response to the scheduled events, and Fargate provides a serverless container execution environment, eliminating the need to provision and manage servers.

解析：Option B, using AWS Batch with AWS Fargate, is the most cost-effective solution. AWS Batch manages the job scheduling and executes the job in response to the scheduled events, and Fargate provides a serverless container execution environment, eliminating the need to provision and manage servers.

417. Question #485A 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?

- 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).

答案：A

解析：Option A, storing the video archives in Amazon S3 Glacier and using Expedited retrievals, is the most cost-effective solution given the requirements. S3 Glacier is a low-cost storage option for long-term archival data. Expedited retrievals can make the archived data available in as fast as 1-5 minutes, which meets the company's requirement for quick access when needed.

解析：Option A, storing the video archives in Amazon S3 Glacier and using Expedited retrievals, is the most cost-effective solution given the requirements. S3 Glacier is a low-cost storage option for long-term archival data. Expedited retrievals can make the archived data available in as fast as 1-5 minutes, which meets the company's requirement for quick access when needed.

418. Question #486A 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?

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.

答案：A

解析: Option A is the most cost-effective and operationally efficient solution. Amazon S3 can be used to host static website content, Amazon ECS with AWS Fargate can manage the containerized logic tier without the need to provision and manage servers, and a managed Amazon RDS cluster can handle the relational database requirements, reducing the operational burden.

解析: Option A is the most cost-effective and operationally efficient solution. Amazon S3 can be used to host static website content, Amazon ECS with AWS Fargate can manage the containerized logic tier without the need to provision and manage servers, and a managed Amazon RDS cluster can handle the relational database requirements, reducing the operational burden.

419. Question #487A 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 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?

- 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

答案: C

解析: Option C, Amazon EFS with multiple mount targets, is the correct solution. Amazon EFS is a scalable file storage service for Amazon EC2 instances that can be accessed on-premises using a Site-to-Site VPN. It supports multiple mount targets, allowing it to be highly available and accessible to multiple Linux instances as a file system.

解析: Option C, Amazon EFS with multiple mount targets, is the correct solution. Amazon EFS is a scalable file storage service for Amazon EC2 instances that can be accessed on-premises using a Site-to-Site VPN. It

supports multiple mount targets, allowing it to be highly available and accessible to multiple Linux instances as a file system.

420. Question #488A 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?
- 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.

答案: C

解析: Option C is the correct solution. A service control policy (SCP) in AWS Organizations allows you to set permissions policies that apply to all accounts in your organization or to specific accounts that you specify. By creating an SCP that denies access to billing information and attaching it to the root OU, you can ensure that no user, including the root user of any member account, can access the billing information.

解析: Option C is the correct solution. A service control policy (SCP) in AWS Organizations allows you to set permissions policies that apply to all accounts in your organization or to specific accounts that you specify. By creating an SCP that denies access to billing information and attaching it to the root OU, you can ensure that no user, including the root user of any member account, can access the billing information.

421. Question #489An 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?

- 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.

答案：C

解析：Option C is the correct solution. By configuring an Amazon SNS dead letter queue with an Amazon SQS target, the undelivered messages can be retained for up to 14 days. This allows for the analysis of messages without additional development effort, as SQS can be used to store the messages with the specified retention period.

解析：Option C is the correct solution. By configuring an Amazon SNS dead letter queue with an Amazon SQS target, the undelivered messages can be retained for up to 14 days. This allows for the analysis of messages without additional development effort, as SQS can be used to store the messages with the specified retention period.

422. Question #490A 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?
- 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.

答案: B

解析: Option B is the correct solution. **DynamoDB provides a feature called point-in-time recovery and continuous backups that can be enabled with minimal configuration.** This feature allows for the automatic backup of the table data to Amazon S3 without affecting the application's availability or the provisioned read capacity units.

解析: Option B is the correct solution. **DynamoDB provides a feature called point-in-time recovery and continuous backups that can be enabled with minimal configuration.** This feature allows for the automatic backup of the table data to Amazon S3 without affecting the application's availability or the provisioned read capacity units.

423. Question #491A 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?**

- 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.

答案：A

解析：Option A is the most cost-effective solution. It uses standard SQS queues, which are less expensive than FIFO queues, while still meeting the requirement to process each request at least once. Using AWS KMS for encryption ensures the security of the credit card data, and adding the kms:Decrypt permission allows the Lambda function to decrypt the messages from the queue.

解析：Option A is the most cost-effective solution. It uses standard SQS queues, which are less expensive than FIFO queues, while still meeting the requirement to process each request at least once. Using AWS KMS for encryption ensures the security of the credit card data, and adding the kms:Decrypt permission allows the Lambda function to decrypt the messages from the queue.

424. Question #492A 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?

- 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.

答案：B

解析：Option B is the solution that requires the least development effort. By using AWS Organizations and SCPs, the company can set up a centralized control over the creation of EC2 instances across multiple accounts. SCPs can be used to restrict the instance types that can be launched, ensuring that staff only uses approved instance types.

解析：Option B is the solution that requires the least development effort. By using AWS Organizations and SCPs, the company can set up a centralized control over the creation of EC2 instances across multiple accounts. SCPs can be used to restrict the instance types that can be launched, ensuring that staff only uses approved instance types.

425. Question #494A 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": ["*"]
        }
    ]
}

```

- 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.

答案: D

解析: The cause of the unsuccessful request is that the IAM policy attached to the administrator's IAM role does not allow the action to terminate the EC2 instance from the source IP address that the administrator is using. The policy likely restricts actions to be

performed only from specific CIDR blocks, and the administrator's request is not coming from one of those allowed IP addresses.

解析: The cause of the unsuccessful request is that the IAM policy attached to the administrator's IAM role does not allow the action to terminate the EC2 instance from the source IP address that the administrator is using. The policy likely restricts actions to be performed only from specific CIDR blocks, and the administrator's request is not coming from one of those allowed IP addresses.

426. Question #495A 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?

- 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.

答案: C

解析: Option C is the correct solution. Amazon Macie is a service that uses machine learning to automatically discover, classify, and protect sensitive data such as PII and financial information in AWS S3 buckets. By running a data discovery job with managed identifiers for specific data types like passport numbers and credit card numbers, the company can identify and protect sensitive data.

解析: Option C is the correct solution. Amazon Macie is a service that uses machine learning to automatically discover, classify, and protect sensitive data such as PII and financial information in AWS S3 buckets. By running a data discovery job with managed identifiers for specific

data types like passport numbers and credit card numbers, the company can identify and protect sensitive data.

427. Question #497A 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?

- 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.

答案: C

解析: Option C is the most cost-effective solution. A VPC gateway endpoint provides a private connection between the VPC and Amazon S3, eliminating the need for a NAT gateway and reducing data transfer costs. The traffic between the VPC and S3 stays within the AWS network, which is more cost-effective than using a NAT gateway.

解析: Option C is the most cost-effective solution. A VPC gateway endpoint provides a private connection between the VPC and Amazon S3, eliminating the need for a NAT gateway and reducing data transfer costs. The traffic between the VPC and S3 stays within the AWS network, which is more cost-effective than using a NAT gateway.

428. Question #498A 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?

- 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.

答案：A

解析：Option A is the solution that will reduce S3 costs with the least operational overhead. S3 Lifecycle policies can be configured to automatically manage object versions, deleting older versions while retaining the two most recent ones. This approach requires minimal manual intervention and leverages S3's built-in capabilities.

解析：Option A is the solution that will reduce S3 costs with the least operational overhead. S3 Lifecycle policies can be configured to automatically manage object versions, deleting older versions while retaining the two most recent ones. This approach requires minimal manual intervention and leverages S3's built-in capabilities.

429. Question #499A 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?

- 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.**

答案: D

解析: Option D is the correct solution. By downgrading to a 200 Mbps hosted connection, the company can significantly reduce the cost of its AWS Direct Connect service. Hosted connections are a more cost-effective option provided by AWS Direct Connect Partners and are suitable for lower utilization rates.

解析: Option D is the correct solution. By downgrading to a 200 Mbps hosted connection, the company can significantly reduce the cost of its AWS Direct Connect service. Hosted connections are a more cost-effective option provided by AWS Direct Connect Partners and are suitable for lower utilization rates.

430. Question #501A 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.

答案: C

解析: Option C is the most operationally efficient solution. Amazon Kinesis Data Firehose can automatically batch, compress, and encrypt the incoming streaming data, and then load it into Amazon S3. Combined with Amazon Kinesis Data Analytics for real-time data analytics, this solution provides a seamless and efficient pipeline for real-time data analysis and ingestion into a data lake.

解析: Option C is the most operationally efficient solution. Amazon Kinesis Data Firehose can automatically batch, compress, and encrypt the incoming streaming data, and then load it into Amazon S3. Combined with Amazon Kinesis Data Analytics for real-time data analytics, this solution provides a seamless and efficient pipeline for real-time data analysis and ingestion into a data lake.

431. Question #503A 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.

答案: A

解析: Option A is the most secure way to grant access. By having customers create an IAM role with a trust policy that allows the company's account to assume that role, the company can obtain temporary credentials to access the customer's account without needing long-term access keys. This approach adheres to the principle of least privilege and is more secure than storing access keys or using other methods that might expose customer credentials.

解析: Option A is the most secure way to grant access. By having customers create an IAM role with a trust policy that allows the company's account to assume that role, the company can obtain temporary credentials to access the customer's account without needing long-term access keys. This approach adheres to the principle of least privilege and is more secure than storing access keys or using other methods that might expose customer credentials.

432. Question #504A 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.

答案: C

解析: Option C is the most operationally efficient solution. AWS Transit Gateway can be used to create a hub-and-spoke architecture where multiple VPCs can be connected to a single Transit Gateway, simplifying network management and reducing the number of peering connections needed. This approach is more efficient than setting up individual VPC peering connections or managing VPN gateways.

解析: Option C is the most operationally efficient solution. AWS Transit Gateway can be used to create a hub-and-spoke architecture where multiple VPCs can be connected to a single Transit Gateway, simplifying network management and reducing the number of peering connections needed. This approach is more efficient than setting up individual VPC peering connections or managing VPN gateways.

433. Question #505A 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.

答案: C

解析: Option C is the most cost-effective solution for batch jobs that run during specific hours. Using Spot Instances can significantly reduce the cost compared to On-Demand instances, as Spot Instances are often available at a discount. Setting a policy to scale out based on CPU usage ensures that the Auto Scaling group can adapt to the workload demands efficiently.

解析: Option C is the most cost-effective solution for batch jobs that run during specific hours. Using Spot Instances can significantly reduce the cost compared to On-Demand instances, as Spot Instances are often available at a discount. Setting a policy to scale out based on CPU usage

ensures that the Auto Scaling group can adapt to the workload demands efficiently.

434. Question #506A 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.

答案: C

解析: Option C is the most scalable solution. By generating presigned URLs for Amazon S3, users can directly upload photos to S3 without the need for intermediate storage on application servers. This approach offloads the upload process to S3, which is designed to handle large volumes of data and can scale automatically to accommodate increases in traffic.

解析: Option C is the most scalable solution. By generating presigned URLs for Amazon S3, users can directly upload photos to S3 without the need for intermediate storage on application servers. This approach offloads the upload process to S3, which is designed to handle large volumes of data and can scale automatically to accommodate increases in traffic.

435. Question #507A 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 central 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.

答案：A

解析：Option A is the recommended solution. Amazon DynamoDB global tables provide a fully managed, multi-region, multi-master database. This allows the company to maintain a single source of truth for the reservation database while providing fast, consistent access to data in multiple geographic locations. DynamoDB's global tables ensure low latency and high performance, meeting the requirement of less than 1 second average latency on updates.

解析：Option A is the recommended solution. Amazon DynamoDB global tables provide a fully managed, multi-region, multi-master database. This allows the company to maintain a single source of truth for the reservation database while providing fast, consistent access to data in multiple geographic locations. DynamoDB's global tables ensure low latency and high performance, meeting the requirement of less than 1 second average

latency on updates.

436. Question #509A 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?

- 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.

答案：B

解析：Option B is the correct action. Network ACLs (Access Control Lists) are the recommended way to control traffic at the subnet level, as they act as a firewall for the subnet. By adding an inbound deny rule to the network ACL for the web tier subnets, the architect can block the illegitimate traffic from the specific IP addresses at the subnet level, which is more efficient than modifying security groups for individual instances.

解析：Option B is the correct action. Network ACLs (Access Control Lists) are the recommended way to control traffic at the subnet level, as they act as a firewall for the subnet. By adding an inbound deny rule to the network ACL for the web tier subnets, the architect can block the illegitimate traffic from the specific IP addresses at the subnet level,

which is more efficient than modifying security groups for individual instances.

437. Question #510A 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?

- 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.

答案: B

解析: Option B is the correct solution. By configuring a VPC peering connection between the two VPCs in different regions, the company can establish a secure and private connection. Updating the subnet route tables ensures proper routing of traffic between the VPCs. Creating 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 allows for secure and specific access to the databases from the application servers.

解析: Option B is the correct solution. By configuring a VPC peering connection between the two VPCs in different regions, the company can establish a secure and private connection. Updating the subnet route tables ensures proper routing of traffic between the VPCs. Creating 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 allows for secure and specific access to the databases from the application servers.

438. Question #511A 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**?

- 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

答案: C

解析: Option C is the most cost-effective solution. Amazon Aurora On-Demand allows developers to use a high-performance database that scales with demand, and they pay only for the compute capacity they use, which is ideal for development environments that are not used continuously. This approach is more cost-effective than provisioning a full-time database instance or using storage solutions that are not designed for database workloads.

解析: Option C is the most cost-effective solution. Amazon Aurora On-Demand allows developers to use a high-performance database that scales with demand, and they pay only for the compute capacity they use, which is ideal for development environments that are not used

continuously. This approach is more cost-effective than provisioning a full-time database instance or using storage solutions that are not designed for database workloads.

439. Question #512A 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?**

- 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.

答案：A

解析：Option A is the solution that requires the least operational overhead. By using AWS Config, the company can automate the process of identifying untagged resources and apply tags to them. Then, these tags can be used in the backup plan to ensure that all resources, including those that were previously untagged, are included in the backup process. This approach reduces manual effort and ensures consistency in the backup strategy.

解析：Option A is the solution that requires the least operational overhead. By using AWS Config, the company can automate the process of identifying untagged resources and apply tags to them. Then, these tags can be used in the backup plan to ensure that all resources, including those that were previously untagged, are included in the backup process. This approach reduces manual effort and ensures consistency in the backup strategy.

440. Question #513A 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?

- 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.

答案：A

解析：Option A is the most suitable solution for the given requirements. Using Amazon S3 in combination with AWS Lambda allows for a serverless architecture that can automatically process and resize images as they are uploaded. This approach is highly scalable and can handle unpredictable traffic patterns without the need for manual intervention. Additionally, storing the resized images in S3 ensures availability and durability.

解析：Option A is the most suitable solution for the given requirements. Using Amazon S3 in combination with AWS Lambda allows for a serverless architecture that can automatically process and resize images as they are uploaded. This approach is highly scalable and can handle unpredictable traffic patterns without the need for manual intervention. Additionally, storing the resized images in S3 ensures availability and durability.

441. Question #514A 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?

- 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.

答案：B

解析：Option B is the correct solution. By creating interface VPC endpoints, the company can ensure that the Amazon EKS control plane is accessed over a private network, maintaining security compliance. Interface VPC endpoints provide a private connection between the Amazon EKS nodes in private subnets and the EKS control plane, allowing the nodes to join the cluster without using public end points.

解析：Option B is the correct solution. By creating interface VPC endpoints, the company can ensure that the Amazon EKS control plane is accessed over a private network, maintaining security compliance. Interface VPC endpoints provide a private connection between the Amazon EKS nodes in private subnets and the EKS control plane, allowing the nodes to join the cluster without using public end points.

442. Question #516A 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?

- 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.

答案：B

解析：Option B is the solution that meets the requirements with the least operational overhead. By using provisioned concurrency with AWS Lambda functions, the company can ensure that there is always a specified amount of concurrency available to process incoming API requests. This helps maintain low latency and consistent response times, even during peak usage times.

解析：Option B is the solution that meets the requirements with the least operational overhead. By using provisioned concurrency with AWS Lambda functions, the company can ensure that there is always a specified amount of concurrency available to process incoming API requests. This helps maintain low latency and consistent response times, even during peak usage times.

443. Question #517A 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?

- 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.

答案：A

解析：Option A is the most operationally efficient solution. AWS Systems Manager supports the ability to directly send session logs to an S3 bucket through the Systems Manager console, which requires minimal setup and ongoing management compared to the other options that involve additional services and configurations.

解析：Option A is the most operationally efficient solution. AWS Systems Manager supports the ability to directly send session logs to an S3 bucket through the Systems Manager console, which requires minimal setup and ongoing management compared to the other options that involve additional services and configurations.

444. Question #518An 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?

- 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

答案：A

解析：Option A is the solution that requires the least amount of effort. Storage autoscaling in Amazon RDS allows the database to automatically increase storage capacity as needed, without the need for manual intervention or causing downtime.

解析: Option A is the solution that requires the least amount of effort. Storage autoscaling in Amazon RDS allows the database to automatically increase storage capacity as needed, without the need for manual intervention or causing downtime.

445. Question #519A 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?

- 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.

答案: B

解析: Option B is the correct solution. AWS Service Catalog allows organizations to create and manage a catalog of products that are approved for use within the organization. Customers can then self-service to deploy these products, which is ideal for centrally managing and providing a common set of solutions and tools.

解析: Option B is the correct solution. AWS Service Catalog allows organizations to create and manage a catalog of products that are approved for use within the organization. Customers can then self-service to deploy these products, which is ideal for centrally managing and providing a common set of solutions and tools.

446. Question #520A 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?

- 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.

答案：B

解析：Option B is the correct answer because **on-demand capacity mode automatically adjusts to your application's read and write requests**. This is cost-effective for unpredictable workloads as it eliminates the need to provision throughput in advance, which can lead to unnecessary costs if the application does not use the full provisioned capacity.

解析：Option B is the correct answer because on-demand capacity mode automatically adjusts to your application's read and write requests. This is cost-effective for unpredictable workloads as it eliminates the need to provision throughput in advance, which can lead to unnecessary costs if the application does not use the full provisioned capacity.

447. Question #521A 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?**

- 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.

答案：C

解析：Option C is the most secure because it uses IAM roles and cross-account access, which allows for fine-grained access control and follows the principle of least privilege. By assuming a role in another account, the inventory application can access the necessary resources without needing long-term credentials that could be compromised. This method also allows for tracking and auditing of access through AWS CloudTrail.

解析：Option C is the most secure because it uses IAM roles and cross-account access, which allows for fine-grained access control and follows the principle of least privilege. By assuming a role in another account, the inventory application can access the necessary resources without needing long-term credentials that could be compromised. This method also allows for tracking and auditing of access through AWS CloudTrail.

448. Question #523A 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?

- A. AWS AppSync pipeline resolvers
- B. Amazon CloudFront with Lambda@Edge functions**
- C. Edge-optimized Amazon API Gateway with AWS Lambda functions
- D. Amazon Athena Federated Query with a DynamoDB connector

答案: B

解析: Option B is the most operationally efficient solution because it leverages Amazon CloudFront's global edge locations to cache and serve data, reducing the load on the DynamoDB tables and decreasing latency for the end-users. Lambda@Edge can be used to execute code at the edge location to customize the content delivery, which in this case can be used to retrieve data from multiple DynamoDB tables.

解析: Option B is the most operationally efficient solution because it leverages Amazon CloudFront's global edge locations to cache and serve data, reducing the load on the DynamoDB tables and decreasing latency for the end-users. Lambda@Edge can be used to execute code at the edge location to customize the content delivery, which in this case can be used to retrieve data from multiple DynamoDB tables.

449. Question #524A 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?

- 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.

答案: C

解析: Option C is the least effort solution because Amazon Athena is a serverless interactive query service that allows users to run SQL-like queries directly against data stored in Amazon S3 where CloudTrail logs are stored. This eliminates the need to set up and manage additional services like AWS Glue or AWS Batch, or to create and maintain custom scripts.

解析: Option C is the least effort solution because Amazon Athena is a serverless interactive query service that allows users to run SQL-like queries directly against data stored in Amazon S3 where CloudTrail logs are stored. This eliminates the need to set up and manage additional services like AWS Glue or AWS Batch, or to create and maintain custom scripts.

450. Question #525A 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?

- 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.

答案: A

解析: Option A is the least operationally intensive as it provides programmatic access to the AWS Cost Explorer data through an API, which can be easily integrated into existing systems or dashboards. Using pagination, the company can retrieve large sets of data without the need for manual downloads or the setup of file transfer protocols, which are more complex and require additional configuration and maintenance.

解析: Option A is the least operationally intensive as it provides programmatic access to the AWS Cost Explorer data through an API, which can be easily integrated into existing systems or dashboards. Using pagination, the company can retrieve large sets of data without the need for manual downloads or the setup of file transfer protocols, which are more complex and require additional configuration and maintenance

451. Question #526A 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?

- 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.

答案: D

解析: Option D is the most efficient solution as Amazon RDS Proxy can help to maintain database connectivity with minimal application downtime during database scaling operations. The proxy automatically manages connections and can direct traffic to the appropriate database instance, whether it's the primary or a read replica, without the need for manual intervention or complex configuration changes.

解析: Option D is the most efficient solution as Amazon RDS Proxy can help to maintain database connectivity with minimal application downtime during database scaling operations. The proxy automatically manages connections and can direct traffic to the appropriate database instance,

whether it's the primary or a read replica, without the need for manual intervention or complex configuration changes.

452. Question #527A 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**?

- 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.

答案: D

解析: Option D provides the most fault tolerance by using an Amazon Aurora global database, which is designed to handle global deployments and provide high availability and disaster recovery across multiple AWS

Regions. By deploying the web and application tiers in a second Region and using Route 53 health checks with a failover routing policy, the company can ensure minimal downtime and a robust, fault-tolerant architecture.

解析: Option D provides the most fault tolerance by using an Amazon Aurora global database, which is designed to handle global deployments and provide high availability and disaster recovery across multiple AWS Regions. By deploying the web and application tiers in a second Region and using Route 53 health checks with a failover routing policy, the company can ensure minimal downtime and a robust, fault-tolerant architecture.

453. Question #528A 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?

- 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.

答案: D

解析: Option D is the most operationally efficient solution as it leverages AWS Lambda for processing the files, which can be triggered directly by S3 event notifications when new files arrive. This serverless approach eliminates the need for managing EC2 instances or job queues, and the Lambda function can be set up to automatically delete the files from S3 once processing is complete, meeting the requirement for minimal operational overhead.

解析: Option D is the most operationally efficient solution as it leverages AWS Lambda for processing the files, which can be triggered directly by S3 event notifications when new files arrive. This serverless approach eliminates the need for managing EC2 instances or job queues, and the Lambda function can be set up to automatically delete the files from S3 once processing is complete, meeting the requirement for minimal operational overhead.

454. Question #529A 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?

- 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.

答案：B

解析：Option B is the correct answer because Amazon RDS provides a managed database service with built-in encryption at rest, which can be enabled using AWS KMS keys. This ensures that sensitive and transactional data is securely encrypted, reducing the operational overhead associated with managing encryption in a self-hosted environment like Amazon EC2 (Option A). Amazon S3 (Option C) is not designed for database workloads, and Amazon CloudWatch Logs (Option D) is for logging and monitoring, not for data encryption.

解析：Option B is the correct answer because Amazon RDS provides a managed database service with built-in encryption at rest, which can be enabled using AWS KMS keys. This ensures that sensitive and transactional data is securely encrypted, reducing the operational overhead associated with managing encryption in a self-hosted environment like Amazon EC2 (Option A). Amazon S3 (Option C) is not designed for database workloads, and Amazon CloudWatch Logs (Option D) is for logging and monitoring, not for data encryption.

455. Question #530A 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?

- 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.

答案：C

解析：Option C is the correct answer because AWS Global Accelerator is designed to improve the performance of applications that are served from multiple AWS Regions by directing user traffic to the optimal endpoint. Global Accelerator can work with NLBs and can reduce latency by routing traffic through the best-performing endpoints based on the user's location. While CloudFront (Option A) and ALBs (Option B) can also improve performance, they do not specifically address the needs of TCP and UDP traffic like Global Accelerator does. Amazon API Gateway (Option D) is more suited for managing and processing incoming API requests rather than optimizing the performance of multiplayer gaming traffic.

解析：Option C is the correct answer because AWS Global Accelerator is designed to improve the performance of applications that are served from multiple AWS Regions by directing user traffic to the optimal endpoint. Global Accelerator can work with NLBs and can reduce latency by routing traffic through the best-performing endpoints based on the user's location. While CloudFront (Option A) and ALBs (Option B) can also improve performance, they do not specifically address the needs of TCP and UDP traffic like Global Accelerator does. Amazon API Gateway (Option D) is more suited for managing and processing incoming API requests rather than optimizing the performance of multiplayer gaming traffic.

456. Question #531A 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?

- 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.

答案：A

解析：Option A is the most operationally efficient solution because AWS Lambda function URLs provide a direct HTTP(S) endpoint to invoke the Lambda function. This allows the third party to call the Lambda function via the provided URL without the need for additional infrastructure or components, which would increase complexity and operational overhead.

解析：Option A is the most operationally efficient solution because AWS Lambda function URLs provide a direct HTTP(S) endpoint to invoke the Lambda function. This allows the third party to call the Lambda function via the provided URL without the need for additional infrastructure or components, which would increase complexity and operational overhead.

457. Question #533A 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?

- 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:isObject/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.

答案：A

解析：Option A is the correct solution because Amazon Macie is specifically designed to discover and protect PII stored in S3. By creating an EventBridge rule to filter SensitiveData events from Macie, the company can automatically detect PII and use SNS to notify the security team. **SQS (Option C and D) is not the best choice for this scenario because it is more suitable for decoupling components in a message-driven architecture rather than for sending alerts to a team.**

解析：Option A is the correct solution because Amazon Macie is specifically designed to discover and protect PII stored in S3. By creating an EventBridge rule to filter SensitiveData events from Macie, the company can automatically detect PII and use SNS to notify the security team. **SQS (Option C and D) is not the best choice for this scenario because it is more suitable for decoupling components in a message-driven architecture rather than for sending alerts to a team.**

458. Question #534A 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?**

- 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.

答案: C

解析: Option C is the most cost-effective solution because it allows the logs to be stored in a cost-efficient storage class after the initial 30 days of high availability are no longer required. S3 Glacier Flexible Retrieval is suitable for data that is infrequently accessed and meets the requirement for 60 days of additional backup retention. An expiration action can then be set to delete the objects after 90 days, aligning with the company's data retention policy.

解析: Option C is the most cost-effective solution because it allows the logs to be stored in a cost-efficient storage class after the initial 30 days of high availability are no longer required. S3 Glacier Flexible Retrieval is suitable for data that is infrequently accessed and meets the requirement for 60 days of additional backup retention. An expiration action can then be set to delete the objects after 90 days, aligning with the company's data retention policy.

459. Question #535A 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?

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.

答案：B

解析：Option B is the correct solution as it enables encryption of Kubernetes secrets in the etcd key-value store using AWS KMS. This directly addresses the requirement to encrypt secrets within the Amazon EKS cluster. Option A, while using AWS KMS, does not encrypt secrets in the etcd store. Option C is unrelated to secret management, and Option D enables EBS volume encryption, which is not relevant to the encryption of Kubernetes secrets.

解析：Option B is the correct solution as it enables encryption of Kubernetes secrets in the etcd key-value store using AWS KMS. This directly addresses the requirement to encrypt secrets within the Amazon EKS cluster. Option A, while using AWS KMS, does not encrypt secrets in the etcd store. Option C is unrelated to secret management, and Option D enables EBS volume encryption, which is not relevant to the encryption of Kubernetes secrets.

460. Question #536A 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?**

- 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.

答案：D

解析：Based on the company's requirements for providing near real-time read-only access to data scientists while ensuring high availability and cost-effectiveness, the most suitable solution is: 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. Here's why this solution is the most appropriate:

1. High Availability: Multi-AZ cluster deployment provides enhanced availability and durability compared to Single-AZ or traditional Multi-AZ instance deployments.
2. Read-Only Access: The two readable standby instances can serve read traffic, allowing data scientists to run their complex queries without affecting the production database.
3. Near Real-Time Access: Multi-AZ clusters use synchronous replication, ensuring that the standby instances are up-to-date with the primary instance.
4. Cost-Effectiveness: This solution is more cost-effective than creating additional read replicas (option C) or scaling up the existing production database (option A).
5. Performance: By distributing read workloads across multiple instances, this setup can handle complex queries from data scientists without impacting the production workload.
6. Scalability: If needed in the future, additional read replicas can be added to the Multi-AZ cluster for further scaling.

To implement this solution:

1. Plan the migration from Single-AZ to Multi-AZ cluster during a maintenance window to minimize downtime.
2. Configure the cluster with appropriate instance sizes to handle both production and data science workloads.
3. Set up read endpoints for the data scientists to connect to the readable standby instances.
4. Implement proper access controls and security groups to ensure data scientists have read-only access.
5. Monitor the cluster performance using Amazon CloudWatch and adjust resources if needed.
6. Educate data scientists on best practices for running complex queries to optimize performance.

Remember to review the official AWS documentation for the most up-to-date information on Multi-AZ cluster deployments and

their specific features and limitations. Sources [1] [Cloud Relational Database - Amazon RDS Features - Amazon Web Services] (<https://aws.amazon.com/rds/features/>) [3] [Improving query performance for RDS for PostgreSQL with Amazon RDS Optimized Reads - Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL_optimizedreads.html) [6] [Working with DB instance read replicas - Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

解析: Based on the company's requirements for providing near real-time read-only access to data scientists while ensuring high availability and cost-effectiveness, the most suitable solution is: 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. Here's why this solution is the most appropriate:

1. High Availability: Multi-AZ cluster deployment provides enhanced availability and durability compared to Single-AZ or traditional Multi-AZ instance deployments.
2. Read-Only Access: The two readable standby instances can serve read traffic, allowing data scientists to run their complex queries without affecting the production database.
3. Near Real-Time Access: Multi-AZ clusters use synchronous replication, ensuring that the standby instances are up-to-date with the primary instance.
4. Cost-Effectiveness: This solution is more cost-effective than creating additional read replicas (option C) or scaling up the existing production database (option A).
5. Performance: By distributing read workloads across multiple instances, this setup can handle complex queries from data scientists without impacting the production workload.
6. Scalability: If needed in the future, additional read replicas can be added to the Multi-AZ cluster for further scaling.

To implement this solution:

1. Plan the migration from Single-AZ to Multi-AZ cluster during a maintenance window to minimize downtime.
2. Configure the cluster with appropriate instance sizes to handle both production and data science workloads.
3. Set up read endpoints for the data scientists to connect to the readable standby instances.
4. Implement proper access controls and security groups to ensure data scientists have read-only access.
5. Monitor the cluster

performance using Amazon CloudWatch and adjust resources if needed. 6. Educate data scientists on best practices for running complex queries to optimize performance. Remember to review the official AWS documentation for the most up-to-date information on Multi-AZ cluster deployments and their specific features and limitations. Sources [1] [Cloud Relational Database - Amazon RDS Features - Amazon Web Services] (<https://aws.amazon.com/rds/features/>) [3] [Improving query performance for RDS for PostgreSQL with Amazon RDS Optimized Reads - Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL_optimizedreads.html) [6] [Working with DB instance read replicas - Amazon Relational Database Service] (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

461. Question #537A 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?

- 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.

答案：A

解析：Option A is the correct solution as it addresses both the need for high availability and the ability to scale. By migrating the MySQL database to Amazon RDS with a Multi-AZ deployment, the database is protected against Availability Zone failures. Using ElastiCache for Redis, which supports data persistence, ensures that session data is stored with high availability. The Auto Scaling group for the web server across three Availability Zones allows the application to scale out as needed to handle increased traffic.

解析：Option A is the correct solution as it addresses both the need for high availability and the ability to scale. By migrating the MySQL database to Amazon RDS with a Multi-AZ deployment, the database is protected against Availability Zone failures. Using ElastiCache for Redis, which supports data persistence, ensures that session data is stored with high availability. The Auto Scaling group for the web server across three Availability Zones allows the application to scale out as needed to handle increased traffic.

462. Question #538A 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?

- 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.

答案: A

解析: Option A is the correct solution as it allows the company to restrict content to specific countries using an allow list. This ensures that only users within the allowed countries can access the content, and a custom error message can be displayed for unauthorized access attempts. Signed URLs (Option B) and encryption (Option C) can provide security but do not geographically restrict content access. Time-restricted access policies (Option D) can control access over time but not by geography.

解析: Option A is the correct solution as it allows the company to restrict content to specific countries using an allow list. This ensures that only users within the allowed countries can access the content, and a custom error message can be displayed for unauthorized access attempts. Signed URLs (Option B) and encryption (Option C) can provide security but do not geographically restrict content access. Time-restricted access policies (Option D) can control access over time but not by geography.

463. Question #539A 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?

- 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.

答案：B

解析：Option B is the correct solution as it provides a cost-effective way to maintain a warm standby SQL Server database in AWS RDS, which can be quickly promoted to primary in the event of a disaster. Using AWS DMS with CDC allows for near real-time data replication, which aligns with the RPO of 30 seconds. This solution is generally more cost-effective than a multi-site active/active setup (Option A), which can be expensive, or running a full pilot light configuration (Option C), which requires keeping a full production-like environment ready at all times.

解析：Option B is the correct solution as it provides a cost-effective way to maintain a warm standby SQL Server database in AWS RDS, which can be quickly promoted to primary in the event of a disaster. Using AWS DMS with CDC allows for near real-time data replication, which aligns with the RPO of 30 seconds. This solution is generally more cost-effective than a multi-site active/active setup (Option A), which can be expensive, or running a full pilot light configuration (Option C), which requires keeping a full production-like environment ready at all times.

464. Question #540A 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?

- 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.

答案：C

解析：Based on the company's requirements for higher availability, improved application performance, and offloading reporting from the primary database system, I recommend using Amazon RDS deployed in a Multi-AZ cluster deployment with an Oracle database. This solution aligns with option C and meets the requirements in the most operationally efficient way. Here's why:

- 1. Higher Availability:
 - Multi-AZ cluster deployment provides enhanced availability and durability compared to single-AZ deployments.
 - It automatically replicates data across multiple Availability Zones, ensuring continuous operation even if an AZ becomes unavailable.
- 2. Improved Application Performance:
 - RDS manages the database infrastructure, allowing the company to focus on application optimization.
 - The Multi-AZ cluster architecture can help distribute read workloads, potentially improving overall performance.
- 3. Offloading Reporting:
 - The reader instance in the Multi-AZ cluster can be used for reporting functions, offloading this work from the primary database.
 - This separation of workloads helps maintain performance for critical transactional operations on the primary instance.
- 4. Operational Efficiency:
 - Amazon RDS automates many database administration tasks, including backups, patching, and hardware scaling.
 - The company can leverage their existing Oracle database expertise, minimizing the learning curve and migration complexity.
- 5. Scalability:
 - RDS allows for easy scaling of compute and storage resources as the company's needs grow.
 - While option D mentions using Amazon Aurora, which is a powerful database engine, it's not the most suitable choice in this scenario because the company is currently using an Oracle database. Migrating from Oracle to Aurora would require additional effort and potential application changes, making it less operationally efficient for this specific use case.
 - To implement this solution, the company should:
 1. Plan the migration from on-premises

Oracle to Amazon RDS for Oracle. 2. Set up the Multi-AZ cluster deployment in Amazon RDS. 3. Migrate the data using AWS Database Migration Service or native Oracle tools. 4. Configure the application to use the new RDS endpoint. 5. Direct reporting functions to use the reader instance in the cluster. Remember to follow AWS best practices for security, such as using VPCs, security groups, and encryption at rest and in transit. Also, ensure that the chosen RDS instance type and storage configuration meet the company's performance requirements. Sources [1] [Migrate an on-premises Oracle database to Amazon RDS for Oracle – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html>) [3] [Replatforming options for Oracle Database – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/replatform-oracle-database-options/replatform-options.html>) [6] [Replatforming backend databases – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-replatforming-costs-applications/replatforming-backend-databases.html>)

解析: Based on the company's requirements for higher availability, improved application performance, and offloading reporting from the primary database system, I recommend using Amazon RDS deployed in a Multi-AZ cluster deployment with an Oracle database. This solution aligns with option C and meets the requirements in the most operationally efficient way. Here's why:

- 1. Higher Availability:
 - Multi-AZ cluster deployment provides enhanced availability and durability compared to single-AZ deployments.
 - It automatically replicates data across multiple Availability Zones, ensuring continuous operation even if an AZ becomes unavailable.
- 2. Improved Application Performance:
 - RDS manages the database infrastructure, allowing the company to focus on application optimization.
 - The Multi-AZ cluster architecture can help distribute read workloads, potentially improving overall performance.
- 3. Offloading Reporting:
 - The reader instance in the Multi-AZ cluster can be used for reporting functions, offloading this work from the primary database.
 - This separation of workloads helps maintain performance for critical transactional operations on the primary

instance.

4. Operational Efficiency:

- Amazon RDS automates many database administration tasks, including backups, patching, and hardware scaling.
- The company can leverage their existing Oracle database expertise, minimizing the learning curve and migration complexity.

5. Scalability:

- RDS allows for easy scaling of compute and storage resources as the company's needs grow. While option D mentions using Amazon Aurora, which is a powerful database engine, it's not the most suitable choice in this scenario because the company is currently using an Oracle database. Migrating from Oracle to Aurora would require additional effort and potential application changes, making it less operationally efficient for this specific use case.

To implement this solution, the company should:

1. Plan the migration from on-premises Oracle to Amazon RDS for Oracle.
2. Set up the Multi-AZ cluster deployment in Amazon RDS.
3. Migrate the data using AWS Database Migration Service or native Oracle tools.
4. Configure the application to use the new RDS endpoint.
5. Direct reporting functions to use the reader instance in the cluster.

Remember to follow AWS best practices for security, such as using VPCs, security groups, and encryption at rest and in transit. Also, ensure that the chosen RDS instance type and storage configuration meet the company's performance requirements.

Sources

- [1] [Migrate an on-premises Oracle database to Amazon RDS for Oracle – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html>)
- [3] [Replatforming options for Oracle Database – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/replatform-oracle-database-options/replatform-options.html>)
- [6] [Replatforming backend databases – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-replatforming-costs-applications/replatforming-backend-databases.html>)

465. Question #542A 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?

- 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.

答案：B

解析：Option B is the correct solution as CloudFront signed URLs provide a secure way to grant temporary access to premium customers. These URLs ensure that only those with the valid signed URL can access the content, and the access is time-limited, which is suitable for on-demand content delivery. Option A is less secure as S3 signed cookies could be more easily shared or compromised. Option C does not provide a mechanism to grant temporary access to specific customers. Option D is not relevant as field-level encryption is more about data security rather than access control.

解析：Option B is the correct solution as CloudFront signed URLs provide a secure way to grant temporary access to premium customers. These URLs ensure that only those with the valid signed URL can access the content, and the access is time-limited, which is suitable for on-demand content delivery. Option A is less secure as S3 signed cookies could be more easily shared or compromised. Option C does not provide a mechanism to grant temporary access to specific customers. Option D is not relevant as field-level encryption is more about data security rather than access control.

466. Question #544A 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?

- 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.

答案: A

解析: Option A is the correct solution as it allows for a gradual rollout of the new API version using a canary release deployment stage. This minimizes impact on customers as it routes only a percentage of the traffic to the new version, allowing for validation before a full deployment. This approach also helps in avoiding data loss as it does not involve overwriting the current production API all at once.

解析: Option A is the correct solution as it allows for a gradual rollout of the new API version using a canary release deployment stage. This minimizes impact on customers as it routes only a percentage of the traffic to the new version, allowing for validation before a full deployment. This approach also helps in avoiding data loss as it does not involve overwriting the current production API all at once.

467. Question #545A 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?

- 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.

答案: B

解析: Option B is the correct solution as it sets up a failover mechanism that requires minimal changes to the existing infrastructure. By using Route 53's active-passive failover configuration, the DNS service can automatically direct users to a static error page hosted on S3 if the health checks for the ALB indicate that it is unhealthy. This ensures high availability with minimal overhead.

解析: Option B is the correct solution as it sets up a failover mechanism that requires minimal changes to the existing infrastructure. By using Route 53's active-passive failover configuration, the DNS service can automatically direct users to a static error page hosted on S3 if the health checks for the ALB indicate that it is unhealthy. This ensures high availability with minimal overhead.

468. Question #546A 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?

- 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.

答案：D

解析：Option D is the correct recommendation as AWS Storage Gateway with iSCSI–VTL interface allows the company to integrate with existing backup applications without major changes. It provides a virtual tape solution that can replace physical tapes, simplifying the backup process and reducing costs associated with tape storage.

解析：Option D is the correct recommendation as AWS Storage Gateway with iSCSI–VTL interface allows the company to integrate with existing backup applications without major changes. It provides a virtual tape solution that can replace physical tapes, simplifying the backup process and reducing costs associated with tape storage.

469. Question #547A 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?

- 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.

答案：A

解析：Option A is the correct solution as Amazon Kinesis Data Firehose is designed to capture, automatically scale, and load streaming data into Amazon S3, making it highly suitable for high-volume data ingestion with minimal operational overhead. AWS Glue (Option B) is more focused on ETL jobs and does not natively support data streaming. AWS Lambda (Option C) could be used for processing streaming data but would require additional setup and management compared to Kinesis Data Firehose. AWS DMS (Option D) is intended for database migration and is not designed for streaming data ingestion.

解析：Option A is the correct solution as Amazon Kinesis Data Firehose is designed to capture, automatically scale, and load streaming data into Amazon S3, making it highly suitable for high-volume data ingestion with minimal operational overhead. AWS Glue (Option B) is more focused on ETL jobs and does not natively support data streaming. AWS Lambda (Option C) could be used for processing streaming data but would require additional setup and management compared to Kinesis Data Firehose. AWS DMS (Option D) is intended for database migration and is not designed for streaming data ingestion.

470. Question #548A 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?

- 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.

答案：B

解析：Option B is the correct solution as it allows for granular control over which services can be used by each department through SCPs, which are a feature of AWS Organizations. This approach requires less operational overhead than manually configuring AWS Systems Manager templates or CloudFormation stacks for each department. AWS Service Catalog (Option D) could also be used to control service usage, but it does not provide the same level of access control as SCPs.

解析：Option B is the correct solution as it allows for granular control over which services can be used by each department through SCPs, which are a feature of AWS Organizations. This approach requires less operational overhead than manually configuring AWS Systems Manager templates or CloudFormation stacks for each department. AWS Service Catalog (Option D) could also be used to control service usage, but it does not provide the same level of access control as SCPs.

471. Question #549A 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?

- 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.

答案：B

解析：Option B is the correct approach as it allows the MySQL cluster in the private subnet to access the internet via a NAT gateway without exposing the database instances to the public internet. This maintains security by keeping the database within the private network while still enabling necessary outbound connections. A NAT instance (Option A) would serve a similar purpose but is less scalable and more complex to manage than a NAT gateway. An internet gateway (Option C) or a virtual private gateway (Option D) would not be appropriate as they would provide public access, which is not desired for a private database cluster.

解析：Option B is the correct approach as it allows the MySQL cluster in the private subnet to access the internet via a NAT gateway without exposing the database instances to the public internet. This maintains security by keeping the database within the private network while still enabling necessary outbound connections. A NAT instance (Option A) would serve a similar purpose but is less scalable and more complex to manage than a NAT gateway. An internet gateway (Option C) or a virtual private gateway (Option D) would not be appropriate as they would provide public access, which is not desired for a private database cluster.

472. Question #551A 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?

- 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.

答案：A

解析：Answer is A Amazon S3 Glacier: Expedited Retrieval: Provides access to data within 1–5 minutes. Standard Retrieval: Provides access to data within 3–5 hours. Bulk Retrieval: Provides access to data within 5–12 hours. Amazon S3 Glacier Deep Archive: Standard Retrieval: Provides access to data within 12 hours. Bulk Retrieval: Provides access to data within 48 hours.

解析：Answer is A Amazon S3 Glacier: Expedited Retrieval: Provides access to data within 1–5 minutes. Standard Retrieval: Provides access to data within 3–5 hours. Bulk Retrieval: Provides access to data within 5–12 hours. Amazon S3 Glacier Deep Archive: Standard Retrieval: Provides access to data within 12 hours. Bulk Retrieval: Provides access to data within 48 hours.

473. Question #552A 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?

- 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. Compute Reserved Instances for a 1-year term.
- D. Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

答案：B

解析：Option B is the correct choice as the No Upfront Compute Savings Plan offers significant savings on compute usage over a 1-year term without requiring a large upfront payment. This provides the flexibility to change EC2 instance types and families as needed every 2–3 months,

which is not possible with Reserved Instances or Savings Plans that require an upfront commitment to specific instance types and families.

解析: Option B is the correct choice as the No Upfront Compute Savings Plan offers significant savings on compute usage over a 1-year term without requiring a large upfront payment. This provides the flexibility to change EC2 instance types and families as needed every 2–3 months, which is not possible with Reserved Instances or Savings Plans that require an upfront commitment to specific instance types and families.

474. Question #553A 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?**

- 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.

答案: A

解析: Option A is the correct solution as Amazon Macie is specifically designed to discover and protect PII by analyzing the data in S3 buckets. It can be configured in each Region to automatically detect and alert on PII, providing the least operational overhead for this task. AWS Security Hub (Option B) is a broader security solution that can integrate with other AWS services but is not specifically designed for PII detection. Amazon Inspector (Option C) is intended for application security assessment, and Amazon GuardDuty (Option D) is focused on detecting malicious activity.

解析: Option A is the correct solution as Amazon Macie is specifically designed to discover and protect PII by analyzing the data in S3 buckets. It can be configured in each Region to automatically detect and alert on PII, providing the least operational overhead for this task. AWS Security

Hub (Option B) is a broader security solution that can integrate with other AWS services but is not specifically designed for PII detection. Amazon Inspector (Option C) is intended for application security assessment, and Amazon GuardDuty (Option D) is focused on detecting malicious activity.

475. Question #554A company's SAP application has a backend SQL Server database in an on-premises environment. The company wants to migrate its on-premises application and database server to AWS. The company needs an instance type that meets the high demands of its SAP database.

On-premises performance data shows that both the SAP application and the database have high memory utilization. Which solution will meet these requirements?

- A. Use the compute optimized instance family for the application. Use the memory optimized instance family for the database.
- B. Use the storage optimized instance family for both the application and the database.
- C. Use the memory optimized instance family for both the application and the database.
- D. Use the high performance computing (HPC) optimized instance family for the application. Use the memory optimized instance family for the database.

答案: C

解析: Option C is the correct solution as memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory, which is suitable for both the SAP application and its SQL Server database with high memory utilization. Compute optimized instances (Option A) are more suited for compute-intensive tasks rather than memory-intensive tasks. Storage optimized instances (Option B) are designed for high I/O workloads, and HPC optimized instances (Option D) are intended for high-performance computing tasks, neither of which aligns with the high memory requirement stated.

解析: Option C is the correct solution as memory optimized instances are designed to deliver fast performance for workloads that process large

data sets in memory, which is suitable for both the SAP application and its SQL Server database with high memory utilization. Compute optimized instances (Option A) are more suited for compute-intensive tasks rather than memory-intensive tasks. Storage optimized instances (Option B) are designed for high I/O workloads, and HPC optimized instances (Option D) are intended for high-performance computing tasks, neither of which aligns with the high memory requirement stated.

476. Question #555A company runs an application in a VPC with public and private subnets. The VPC extends across multiple Availability Zones. The application runs on **Amazon EC2 instances in private subnets**. The application uses an Amazon Simple Queue Service (Amazon SQS) queue. A solutions architect needs to design **a secure solution to establish a connection between the EC2 instances and the SQS queue**. Which solution will meet these requirements?

- A. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.
- B. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach to the interface endpoint a VPC endpoint policy that allows access from the EC2 instances that are in the private subnets.
- C. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach an Amazon SQS access policy to the interface VPC endpoint that allows requests from only a specified VPC endpoint.
- D. Implement a gateway VPC endpoint for Amazon SQS. Add a NAT gateway to the private subnets. Attach an IAM role to the EC2 instances that allows access to the SQS queue.

答案：A

解析：Option A is the correct solution as it allows the EC2 instances in the private subnets to communicate with Amazon SQS using a VPC endpoint that resides in the private subnet. This ensures that the traffic between

the EC2 instances and SQS stays within the VPC and does not go over the public internet, enhancing security. Adding a security group with an inbound rule allows only the necessary traffic from the EC2 instances to reach the SQS endpoint. A gateway VPC endpoint (Option D) is not available for Amazon SQS, and configuring the endpoint to use public subnets (Options B and C) would expose the traffic to the public internet, which is not desired for a secure connection.

解析: Option A is the correct solution as it allows the EC2 instances in the private subnets to communicate with Amazon SQS using a VPC endpoint that resides in the private subnet. This ensures that the traffic between the EC2 instances and SQS stays within the VPC and does not go over the public internet, enhancing security. Adding a security group with an inbound rule allows only the necessary traffic from the EC2 instances to reach the SQS endpoint. A gateway VPC endpoint (Option D) is not available for Amazon SQS, and configuring the endpoint to use public subnets (Options B and C) would expose the traffic to the public internet, which is not desired for a secure connection.

477. Question #556A solutions architect is using an AWS CloudFormation template to deploy a three-tier web application. The web application consists of a web tier and an application tier that stores and retrieves user data in Amazon DynamoDB tables. The web and application tiers are hosted on Amazon EC2 instances, and the database tier is not publicly accessible. The application EC2 instances need to access the DynamoDB tables without exposing API credentials in the template. What should the solutions architect do to meet these requirements?

- A. Create an IAM role to read the DynamoDB tables. Associate the role with the application instances by referencing an instance profile.
- B. Create an IAM role that has the required permissions to read and write from the DynamoDB tables. Add the role to the EC2 instance profile, and associate the instance profile with the application instances.
- C. Use the parameter section in the AWS CloudFormation template to have the user input access and secret keys from an already-created IAM user that has the required permissions to read and write from the DynamoDB

tables.

D. Create an IAM user in the AWS CloudFormation template that has the required permissions to read and write from the DynamoDB tables. Use the GetAtt function to retrieve the access and secret keys, and pass them to the application instances through the user data.

答案：B

解析：Option B is the correct approach as it involves creating an IAM role with the necessary permissions for the EC2 instances to access the DynamoDB tables. This role is then added to an EC2 instance profile, which is associated with the application instances. This ensures that the application instances can access the DynamoDB tables without exposing API credentials in the CloudFormation template. Option A is incorrect because it only allows read access, which does not align with the requirement to store and retrieve user data. Option C and D are not secure practices as they involve user input of credentials or passing credentials through user data, which could lead to exposure of sensitive information.

解析：Option B is the correct approach as it involves creating an IAM role with the necessary permissions for the EC2 instances to access the DynamoDB tables. This role is then added to an EC2 instance profile, which is associated with the application instances. This ensures that the application instances can access the DynamoDB tables without exposing API credentials in the CloudFormation template. Option A is incorrect because it only allows read access, which does not align with the requirement to store and retrieve user data. Option C and D are not secure practices as they involve user input of credentials or passing credentials through user data, which could lead to exposure of sensitive information.

478. Question #557A solutions architect manages an analytics application. The application stores large amounts of semistructured data in an Amazon S3 bucket. The solutions architect wants to use parallel data processing to process the data more quickly. The solutions architect also wants to use information that is stored in an Amazon Redshift database to enrich the data. Which solution will meet these requirements?

- A. Use Amazon Athena to process the S3 data. Use AWS Glue with the Amazon Redshift data to enrich the S3 data.
- B. Use Amazon EMR to process the S3 data. Use Amazon EMR with the Amazon Redshift data to enrich the S3 data.**
- C. Use Amazon EMR to process the S3 data. Use Amazon Kinesis Data Streams to move the S3 data into Amazon Redshift so that the data can be enriched.
- D. Use AWS Glue to process the S3 data. Use AWS Lake Formation with the Amazon Redshift data to enrich the S3 data.

答案：B

解析：Option B is the correct solution as Amazon EMR can process large amounts of data in parallel using its Hadoop-based framework, which is suitable for semistructured data stored in S3. Additionally, EMR can directly integrate with Amazon Redshift to enrich the data by querying and joining it with the data stored in S3. This provides a powerful and flexible way to analyze and enrich data at scale.

解析：Option B is the correct solution as Amazon EMR can process large amounts of data in parallel using its Hadoop-based framework, which is suitable for semistructured data stored in S3. Additionally, EMR can directly integrate with Amazon Redshift to enrich the data by querying and joining it with the data stored in S3. This provides a powerful and flexible way to analyze and enrich data at scale.

479. Question #558A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month. What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.

- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

答案: C

解析: Option C is the most cost-effective solution as VPC peering provides a direct and private connection between the two VPCs within the same region and AWS account without incurring data transfer charges. This is ideal for small to moderate amounts of data transfer, which aligns with the scenario described. AWS Transit Gateway (Option A) and AWS Site-to-Site VPN (Option B) would incur additional costs for setup and operation. AWS Direct Connect (Option D) is a more expensive solution that is typically used for larger data transfer needs and requires dedicated connections.

解析: Option C is the most cost-effective solution as VPC peering provides a direct and private connection between the two VPCs within the same region and AWS account without incurring data transfer charges. This is ideal for small to moderate amounts of data transfer, which aligns with the scenario described. AWS Transit Gateway (Option A) and AWS Site-to-Site VPN (Option B) would incur additional costs for setup and operation. AWS Direct Connect (Option D) is a more expensive solution that is typically used for larger data transfer needs and requires dedicated connections.

480. Question #560A 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. Which solution will meet these requirements with the LEAST operational overhead?

- 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.

答案：A

解析: old (C) -->new (A) old: The use of AWS Service Catalog to create accounts in Organizations (Option C) combined with an AWS CloudTrail organization trail is a cost-effective solution for monitoring and alerting on changes to the OU hierarchy. CloudTrail provides a record of all changes made in the AWS account, including changes to the OU structure, with minimal operational overhead. AWS Control Tower (Options A and B) offers additional features for managing accounts and resources but may introduce more complexity and overhead than necessary for simply monitoring OU changes. AWS CloudFormation (Option D) is not designed for monitoring changes to AWS resource hierarchies.

解析: old (C) -->new (A) old: The use of AWS Service Catalog to create accounts in Organizations (Option C) combined with an AWS CloudTrail organization trail is a cost-effective solution for monitoring and alerting on changes to the OU hierarchy. CloudTrail provides a record of all changes made in the AWS account, including changes to the OU structure, with minimal operational overhead. AWS Control Tower (Options A and B) offers additional features for managing accounts and resources but may introduce more complexity and overhead than necessary for simply monitoring OU changes. AWS CloudFormation (Option D) is not designed for monitoring changes to AWS resource hierarchies.

481. Question #561A 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?**

- 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.

答案：A

解析：Option A, setting up a DynamoDB Accelerator (DAX) cluster, is the correct solution as DAX is specifically designed to cache frequently accessed items from DynamoDB, reducing the latency of read operations. Routing all read requests through DAX requires minimal changes to the existing application architecture and provides a scalable solution with low operational overhead. Options B and C involve setting up and managing an ElastiCache layer, which requires additional operational overhead for maintenance and potential synchronization issues. Option D introduces a more complex solution with DynamoDB Streams and AWS Lambda, which increases operational overhead due to the need for managing event-driven architectures.

解析：Option A, setting up a DynamoDB Accelerator (DAX) cluster, is the correct solution as DAX is specifically designed to cache frequently accessed items from DynamoDB, reducing the latency of read operations. Routing all read requests through DAX requires minimal changes to the existing application architecture and provides a scalable solution with low operational overhead. Options B and C involve setting up and managing an ElastiCache layer, which requires additional operational overhead for maintenance and potential synchronization issues. Option D introduces a more complex solution with DynamoDB Streams and AWS Lambda, which increases operational overhead due to the need for managing event-driven

architectures.

482. Question #563A 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?**

- 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.

答案：B

解析：Option B, using Amazon EKS Connector, is the solution that meets the requirement with the least operational overhead. The EKS Connector allows the registration and connection of all Kubernetes clusters, including on-premises clusters, to the Amazon EKS control plane. This provides a unified view of all clusters and workloads from the Amazon EKS console without the need for extensive configuration or management overhead.

解析：Option B, using Amazon EKS Connector, is the solution that meets the requirement with the least operational overhead. The EKS Connector allows the registration and connection of all Kubernetes clusters, including on-premises clusters, to the Amazon EKS control plane. This provides a unified view of all clusters and workloads from the Amazon EKS console without the need for extensive configuration or management overhead.

483. Question #564A 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?

- 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.

答案：B

解析：Option B is the correct solution as it involves using Amazon RDS for MySQL with AWS KMS for client-side encryption. **This ensures that sensitive data is encrypted before it is sent to the database,** and the encryption keys are managed by AWS KMS. This approach provides a high level of security as the data is encrypted at rest and in transit, and access to the encryption keys can be tightly controlled, limiting access even by database administrators.

解析：Option B is the correct solution as it involves using Amazon RDS for MySQL with AWS KMS for client-side encryption. This ensures that sensitive data is encrypted before it is sent to the database, and the encryption keys are managed by AWS KMS. This approach provides a high level of security as the data is encrypted at rest and in transit, and access to the encryption keys can be tightly controlled, limiting access even by database administrators.

484. Question #565A 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?

- 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.

答案：C

解析：Option C is the correct solution as it involves using AWS DMS to migrate the MySQL database to Amazon Aurora, which is a MySQL-compatible relational database. Aurora supports automatic scaling to adjust capacity during periods of increased demand, ensuring that the database can handle transactional workloads efficiently. This option maintains application compatibility and provides the required scalability.

解析：Option C is the correct solution as it involves using AWS DMS to migrate the MySQL database to Amazon Aurora, which is a MySQL-compatible relational database. Aurora supports automatic scaling to adjust capacity during periods of increased demand, ensuring that the database can handle transactional workloads efficiently. This option maintains application compatibility and provides the required scalability.

485. Question #566A 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?

- 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.

答案：B

解析：Option B is the correct solution as Amazon EFS provides a scalable, elastic file system that can be accessed by multiple EC2 instances concurrently. It supports a hierarchical directory structure and allows for rapid read and write access, which is necessary for the applications described. EFS can be mounted on each EC2 instance, providing shared storage that meets the requirements. Amazon S3 (Option A) is not suitable for this use case as it does not support the same level of file system operations. Attaching a single EBS volume (Option C) would not provide concurrent access, and synchronizing EBS volumes (Option D) across instances would require additional management and could introduce complexity and potential for data inconsistency.

解析：Option B is the correct solution as Amazon EFS provides a scalable, elastic file system that can be accessed by multiple EC2 instances concurrently. It supports a hierarchical directory structure and allows for rapid read and write access, which is necessary for the applications described. EFS can be mounted on each EC2 instance, providing shared storage that meets the requirements. Amazon S3 (Option A) is not suitable for this use case as it does not support the same level of file system operations. Attaching a single EBS volume (Option C) would not provide concurrent access, and synchronizing EBS volumes (Option D) across instances would require additional management and could introduce complexity and potential for data inconsistency.

486. Question #567A 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?

- 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.

答案：A

解析：Option A is the correct solution as it leverages Amazon API Gateway and AWS Lambda, both of which are managed services that require minimal operational overhead. This serverless architecture allows for the processing and storage of data from sensors without the need to manage EC2 instances or file systems. Storing the data in Amazon DynamoDB provides a scalable and flexible NoSQL database solution that can handle the workload's needs and future feature additions.

解析：Option A is the correct solution as it leverages Amazon API Gateway and AWS Lambda, both of which are managed services that require minimal operational overhead. This serverless architecture allows for the processing and storage of data from sensors without the need to manage EC2 instances or file systems. Storing the data in Amazon DynamoDB provides a scalable and flexible NoSQL database solution that can handle the workload's needs and future feature additions.

487. Question #568A 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?

- 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

答案: A

解析: Option A is the correct solution as Amazon S3 provides highly durable and scalable object storage capable of storing petabytes of data, and Amazon CloudFront can be used as a caching layer to improve the load times for the engineering drawings. This combination offers a balance of cost, performance, and scalability that meets the requirements for storing large amounts of data and providing fast access to users.

解析: Option A is the correct solution as Amazon S3 provides highly durable and scalable object storage capable of storing petabytes of data, and Amazon CloudFront can be used as a caching layer to improve the load times for the engineering drawings. This combination offers a balance of cost, performance, and scalability that meets the requirements for storing large amounts of data and providing fast access to users.

488. Question #569An 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?

- 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.

答案: A

解析: Option A is the correct solution as Amazon CloudWatch provides metrics for EventBridge that can be used to determine if the rule conditions are met and if the target is being invoked. These metrics would show the number of events that matched the rule and the number of times the target was invoked, allowing the solutions architect to verify the behavior of the EventBridge rule.

解析: Option A is the correct solution as Amazon CloudWatch provides metrics for EventBridge that can be used to determine if the rule conditions are met and if the target is being invoked. These metrics would show the number of events that matched the rule and the number of times the target was invoked, allowing the solutions architect to verify the behavior of the EventBridge rule.

489. Question #570A 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?

- 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.

答案: B

解析: Option B is the correct solution as it allows the company to set up a scheduled action in an Auto Scaling group to automatically scale up to six instances every Friday evening and scale down to the normal capacity afterward. This approach requires minimal operational overhead as it does not require manual intervention each week. Amazon EventBridge reminders (Option A) would require manual actions, and both manual scaling (Option C) and automatic scaling (Option D) without a scheduled action would not ensure the scaling happens reliably every week as needed.

解析: Option B is the correct solution as it allows the company to set up a scheduled action in an Auto Scaling group to automatically scale up to six instances every Friday evening and scale down to the normal capacity afterward. This approach requires minimal operational overhead as it does not require manual intervention each week. Amazon EventBridge reminders (Option A) would require manual actions, and both manual scaling (Option C) and automatic scaling (Option D) without a scheduled action would not ensure the scaling happens reliably every week as needed.

490. Question #571A 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?

- 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.

答案: B

解析: Option B is the correct solution. AWS Certificate Manager (ACM) allows the creation of a certificate that can be signed by a third-party CA, meeting the company's requirement for a specific public third-party CA. Once the certificate is created in ACM, it can be used to configure a custom domain in Amazon API Gateway, which supports TLSv1.3. This ensures

that the API endpoints use the required TLS version and the certificate signed by the specified CA.

解析: Option B is the correct solution. AWS Certificate Manager (ACM) allows the creation of a certificate that can be signed by a third-party CA, meeting the company's requirement for a specific public third-party CA. Once the certificate is created in ACM, it can be used to configure a custom domain in Amazon API Gateway, which supports TLSv1.3. This ensures that the API endpoints use the required TLS version and the certificate signed by the specified CA.

491. Question #572A 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**?

- 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.

答案: C

解析: Option C, Amazon Aurora Serverless v2, is the correct solution as it offers a serverless option for Aurora databases, which automatically scales compute resources based on the workload without requiring manual intervention. This aligns with the company's need for a managed service with auto scaling capabilities and minimal administrative overhead.

DynamoDB (Option A) does not meet the MySQL compatibility requirement. A provisioned Aurora database (Option B) and an RDS for MySQL database (Option D) would require manual scaling actions to adjust capacity.

解析: Option C, Amazon Aurora Serverless v2, is the correct solution as it offers a serverless option for Aurora databases, which automatically scales compute resources based on the workload without requiring manual intervention. This aligns with the company's need for a managed service with auto scaling capabilities and minimal administrative overhead. DynamoDB (Option A) does not meet the MySQL compatibility requirement. A provisioned Aurora database (Option B) and an RDS for MySQL database (Option D) would require manual scaling actions to adjust capacity.

492. Question #573A 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?

- 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.

答案: D

解析: Option D, Lambda SnapStart, is the correct solution as it is designed to reduce the impact of cold starts for Lambda functions running on Java 11. SnapStart is a feature that can improve the startup time of Lambda functions by up to 90% at no additional cost. This makes it a cost-effective solution for reducing latency when compared to provisioned concurrency (Option A), which incurs additional costs for maintaining a certain number of instances ready to respond. Increasing the timeout (Option B) and memory (Option C) do not directly address the issue of startup latency.

解析: Option D, Lambda SnapStart, is the correct solution as it is designed to reduce the impact of cold starts for Lambda functions running on Java 11. SnapStart is a feature that can improve the startup time of Lambda functions by up to 90% at no additional cost. This makes it a cost-effective solution for reducing latency when compared to provisioned

concurrency (Option A), which incurs additional costs for maintaining a certain number of instances ready to respond. Increasing the timeout (Option B) and memory (Option C) do not directly address the issue of startup latency.

493. Question #574A 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**?

- 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.

答案：A

解析：Option A, Aurora Serverless v2, **is the most cost-effective solution for a workload with highly variable and intermittent usage patterns**. It automatically scales down to zero when not in use and charges per second for the time the database is active, which is ideal for an application that only runs for 2 hours a week. This minimizes costs compared to the other options, which would either incur higher running costs (Option B, C) or require more management and potential additional costs (Option D).

解析：Option A, Aurora Serverless v2, **is the most cost-effective solution for a workload with highly variable and intermittent usage patterns**. It automatically scales down to zero when not in use and charges per second for the time the database is active, which is ideal for an application that only runs for 2 hours a week. This minimizes costs compared to the other options, which would either incur higher running costs (Option B,

C) or require more management and potential additional costs (Option D).

494. Question #575A 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**?

- 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.

答案：C

解析：Option C, a Multi-AZ DB cluster deployment in Amazon RDS, is the most operationally efficient solution. It provides high availability and automatic failover within a single AWS Region by replicating data across multiple Availability Zones. Additionally, it can be configured to increase read capacity by adding read replicas, which can help with the increased read workloads without compromising on the operational efficiency. DynamoDB (Option A) does not provide the same level of relational database features as PostgreSQL, and while Multi-AZ deployments (Option B) offer high availability, they do not inherently increase read capacity. Cross-Region read replicas (Option D) would increase read capacity, but they add complexity and latency due to cross-Region replication.

解析：Option C, a Multi-AZ DB cluster deployment in Amazon RDS, is the most operationally efficient solution. It provides high availability and automatic failover within a single AWS Region by replicating data across multiple Availability Zones. Additionally, it can be configured to increase read capacity by adding read replicas, which can help with the increased read workloads without compromising on the operational

efficiency. DynamoDB (Option A) does not provide the same level of relational database features as PostgreSQL, and while Multi-AZ deployments (Option B) offer high availability, they do not inherently increase read capacity. Cross-Region read replicas (Option D) would increase read capacity, but they add complexity and latency due to cross-Region replication.

495. Question #576A 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?

- A. Private endpoint
- B. Regional endpoint
- C. Interface VPC endpoint
- D. Edge-optimized endpoint

答案: D

解析: Option D, an edge-optimized endpoint, is the most suitable choice for a geographically distributed user base. This is because edge-optimized endpoints route requests through the CloudFront Edge locations, which are distributed globally, thereby improving latency by bringing the service closer to the users. Private and regional endpoints are more suitable for internal or local traffic, respectively, while an interface VPC endpoint is used for allowing resources within a VPC to communicate with AWS services.

解析: Option D, an edge-optimized endpoint, is the most suitable choice for a geographically distributed user base. This is because edge-optimized endpoints route requests through the CloudFront Edge locations, which are distributed globally, thereby improving latency by bringing the service closer to the users. Private and regional endpoints are more suitable for internal or local traffic, respectively, while an interface VPC endpoint is used for allowing resources within a VPC to communicate with AWS services.

496. Question #577A 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?

- 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.

答案：C

解析：Option C is the most operationally efficient solution. AWS Certificate Manager (ACM) can automate the creation and renewal of TLS certificates, and using DNS validation for domain verification eliminates the need for manual intervention. This process is integrated and streamlined, reducing the administrative overhead compared to email validation, which requires manual approval of each validation email.

解析：Option C is the most operationally efficient solution. AWS Certificate Manager (ACM) can automate the creation and renewal of TLS certificates, and using DNS validation for domain verification eliminates the need for manual intervention. This process is integrated and streamlined, reducing the administrative overhead compared to email validation, which requires manual approval of each validation email.

497. Question #578A 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?

- 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.

答案：A

解析：Option A, DynamoDB Accelerator (DAX), is a fully managed, highly available, in-memory cache for Amazon DynamoDB that can significantly improve database response times from milliseconds to microseconds. This solution requires minimal operational overhead as it is a managed service that integrates seamlessly with DynamoDB. Migrating to Amazon Redshift or Amazon RDS would not be as efficient in terms of performance for a serverless application, and setting up Amazon ElastiCache for Redis would involve additional management and configuration.

解析：Option A, DynamoDB Accelerator (DAX), is a fully managed, highly available, in-memory cache for Amazon DynamoDB that can significantly improve database response times from milliseconds to microseconds. This solution requires minimal operational overhead as it is a managed service that integrates seamlessly with DynamoDB. Migrating to Amazon Redshift or Amazon RDS would not be as efficient in terms of performance for a serverless application, and setting up Amazon ElastiCache for Redis would involve additional management and configuration.

498. Question #579A 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?

- 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.

答案：A

解析: Option A, using the Instance Scheduler on AWS, allows the company to automate the start and stop of the RDS instance according to a predefined schedule that aligns with business hours. This minimizes costs by only running the database when it is needed and reduces operational overhead by eliminating the need for manual intervention. Turning off automatic backups and creating manual snapshots (Option B) could risk data integrity and compliance issues. Creating a custom AWS Lambda function (Option C) would require additional development and maintenance. Purchasing All Upfront reserved DB instances (Option D) may not be cost-effective given the intermittent usage pattern.

解析: Option A, using the Instance Scheduler on AWS, allows the company to automate the start and stop of the RDS instance according to a predefined schedule that aligns with business hours. This minimizes costs by only running the database when it is needed and reduces operational overhead by eliminating the need for manual intervention. Turning off automatic backups and creating manual snapshots (Option B) could risk data integrity and compliance issues. Creating a custom AWS Lambda function (Option C) would require additional development and maintenance. Purchasing All Upfront reserved DB instances (Option D) may not be cost-effective given the intermittent usage pattern.

499. Question #580A 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**?

- 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.

答案: D

解析: Option D, using an Amazon EBS GP3 volume, is the most cost-effective solution for running latency-sensitive applications on Amazon EC2 instances. GP3 volumes offer high performance at a lower cost compared to GP2 volumes (Option B) and do not require changes to the application architecture, making them suitable for a lift and shift migration. Amazon FSx for Lustre (Option A) and OpenZFS (Option C) are high-performance file systems that may be more expensive and could require application changes.

解析: Option D, using an Amazon EBS GP3 volume, is the most cost-effective solution for running latency-sensitive applications on Amazon EC2 instances. GP3 volumes offer high performance at a lower cost compared to GP2 volumes (Option B) and do not require changes to the application architecture, making them suitable for a lift and shift migration. Amazon FSx for Lustre (Option A) and OpenZFS (Option C) are high-performance file systems that may be more expensive and could require application changes.

500. Question #581A 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?

- 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.

答案：B

解析：Option B is the correct choice for ensuring high availability and fault tolerance. By setting the Auto Scaling group's minimum capacity to four and deploying two On-Demand Instances in each of two different Availability Zones, the architect ensures that there are always at least two running instances in each AZ. This configuration protects against the failure of an entire AZ and provides the necessary redundancy to maintain application availability.

解析：Option B is the correct choice for ensuring high availability and fault tolerance. By setting the Auto Scaling group's minimum capacity to four and deploying two On-Demand Instances in each of two different Availability Zones, the architect ensures that there are always at least two running instances in each AZ. This configuration protects against the failure of an entire AZ and provides the necessary redundancy to maintain application availability.

501. Question #582An 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?

- 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.

答案：A

解析：Option A, setting up a geolocation routing policy, is the most effective solution for minimizing load time. Geolocation routing directs users to the nearest endpoint based on their geographic location, which in this case would be the on-premises data center for users near us-west-1 and the AWS Cloud in eu-central-1 for users in that region. This approach reduces latency by ensuring users are connected to the closest server, providing a faster loading experience.

解析：Option A, setting up a geolocation routing policy, is the most effective solution for minimizing load time. Geolocation routing directs users to the nearest endpoint based on their geographic location, which in this case would be the on-premises data center for users near us-west-1 and the AWS Cloud in eu-central-1 for users in that region. This approach reduces latency by ensuring users are connected to the closest server, providing a faster loading experience.

502. Question #583A 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?

- 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.

答案：C

解析: Option C, using AWS Snowball with Tape Gateway, is the most cost-effective solution for migrating large amounts of archived data to AWS, especially when considering the limited bandwidth of 1 Gbps. Snowball devices allow for physical transfer of data, which is faster and more cost-effective than transferring 5 PB of data over the internet. Once the data is in AWS, a lifecycle policy can move the data to Amazon S3 Glacier Deep Archive for long-term storage, meeting the company's compliance needs.

解析: Option C, using AWS Snowball with Tape Gateway, is the most cost-effective solution for migrating large amounts of archived data to AWS, especially when considering the limited bandwidth of 1 Gbps. Snowball devices allow for physical transfer of data, which is faster and more cost-effective than transferring 5 PB of data over the internet. Once the data is in AWS, a lifecycle policy can move the data to Amazon S3 Glacier Deep Archive for long-term storage, meeting the company's compliance needs.

503. Question #584A 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?

- 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.

答案: A

解析: Option A, running the EC2 instances in a spread placement group, ensures that the instances are placed on distinct physical hardware, which helps to prevent correlated failures and meets the requirement of not sharing the same underlying hardware. This is a more cost-effective solution compared to configuring dedicated tenancy (Option C), which may incur higher costs and is not necessary for simply preventing groups of nodes from sharing hardware. Options B and D do not address the

requirement of preventing hardware sharing.

解析: Option A, running the EC2 instances in a spread placement group, ensures that the instances are placed on distinct physical hardware, which helps to prevent correlated failures and meets the requirement of not sharing the same underlying hardware. This is a more cost-effective solution compared to configuring dedicated tenancy (Option C), which may incur higher costs and is not necessary for simply preventing groups of nodes from sharing hardware. Options B and D do not address the requirement of preventing hardware sharing.

504. Question #585A 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?

- 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.

答案: D

解析: Option D, **purchasing a Capacity Reservation in the failover Region**, ensures that the necessary EC2 capacity is reserved and available when needed, which is critical for a disaster recovery strategy. This guarantees that the required compute capacity is met without competition for available instances. On-Demand Instances (Option A) do not reserve capacity, and while Savings Plans (Option B) and Reserved Instances (Option C) offer cost savings, they do not guarantee capacity in the event of a disaster.

解析: Option D, **purchasing a Capacity Reservation in the failover Region**, ensures that the necessary EC2 capacity is reserved and available when needed, which is critical for a disaster recovery strategy. This guarantees that the required compute capacity is met without competition for available instances. On-Demand Instances (Option A) do not reserve capacity, and while Savings Plans (Option B) and Reserved Instances (Option C) offer cost savings, they do not guarantee capacity in the

event of a disaster.

505. Question #586A 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?

- 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.

答案: B

解析: Option B is the correct next step. The solutions architect should invite the R&D; AWS account to be part of the new organization after the R&D; AWS account has been removed from the prior organization. This ensures a clean separation and transition for the R&D; business unit into its own management account within AWS Organizations. Creating a new account (Option C) is unnecessary if the existing R&D; account can be transferred. Options A and D do not provide the clean break required for the R&D; business to have its own separate organization.

解析: Option B is the correct next step. The solutions architect should invite the R&D; AWS account to be part of the new organization after the R&D; AWS account has been removed from the prior organization. This ensures a clean separation and transition for the R&D; business unit into its own management account within AWS Organizations. Creating a new account (Option C) is unnecessary if the existing R&D; account can be transferred. Options A and D do not provide the clean break required for the R&D; business to have its own separate organization.

506. Question #587A 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?

- 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.

答案: C

解析: Option C is the solution that best meets the requirements. **Amazon API Gateway can act as a front end to various services, providing an authorization layer through Lambda authorizers.** Amazon Kinesis Data Firehose is a fully managed service that can capture and automatically load streaming data into data lakes, analytics tools, and machine learning models, making it suitable for unpredictable and increasing customer activity. Storing the received information in Amazon S3 ensures durability and accessibility for further processing.

解析: Option C is the solution that best meets the requirements. Amazon API Gateway can act as a front end to various services, providing an authorization layer through Lambda authorizers. Amazon Kinesis Data Firehose is a fully managed service that can capture and automatically load streaming data into data lakes, analytics tools, and machine learning models, making it suitable for unpredictable and increasing customer activity. Storing the received information in Amazon S3 ensures durability and accessibility for further processing.

507. Question #588An 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?

- 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.**

答案: D

解析: Option D, copying automatic snapshots to another Region every 24 hours, is the most cost-effective solution. This approach aligns with the company's RPO and RTO of 24 hours and leverages the built-in snapshot functionality of Amazon RDS without incurring additional service costs or the complexity of setting up replication. Cross-Region read replicas (Option A) and AWS DMS (Option B) are more expensive due to the continuous replication and management overhead. Option C, while also leveraging S3, would require additional setup and management compared to leveraging RDS's automatic snapshot capability.

解析: Option D, copying automatic snapshots to another Region every 24 hours, is the most cost-effective solution. This approach aligns with the company's RPO and RTO of 24 hours and leverages the built-in snapshot

functionality of Amazon RDS without incurring additional service costs or the complexity of setting up replication. Cross-Region read replicas (Option A) and AWS DMS (Option B) are more expensive due to the continuous replication and management overhead. Option C, while also leveraging S3, would require additional setup and management compared to leveraging RDS's automatic snapshot capability.

508. Question #589A 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?

- 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.

答案：B

解析：Option B, using Amazon ElastiCache for Redis, is the solution that meets the requirements for high availability and session state persistence. Redis provides data structures such as strings, hashes, lists, sets, and sorted sets, which can be used to store session state data. Moreover, Redis offers high availability and failover capabilities, which ensures that the session state is not lost in the event of a web server outage. This is in contrast to Memcached (Option A), which is more of an in-memory caching system and does not provide the same level of persistence and data management capabilities as Redis. Options C and D are not designed for session state management and would not provide the

necessary high availability guarantees.

解析: Option B, using Amazon ElastiCache for Redis, is the solution that meets the requirements for high availability and session state persistence. Redis provides data structures such as strings, hashes, lists, sets, and sorted sets, which can be used to store session state data. Moreover, Redis offers high availability and failover capabilities, which ensures that the session state is not lost in the event of a web server outage. This is in contrast to Memcached (Option A), which is more of an in-memory caching system and does not provide the same level of persistence and data management capabilities as Redis. Options C and D are not designed for session state management and would not provide the necessary high availability guarantees.

509. Question #590A 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?

- 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.

答案: A

解析: Option A, creating a read replica of the database, is the most effective solution for maintaining performance during periodic heavy reporting workloads. The read replica can handle the additional query load, thus preventing a slowdown of the primary database that serves the daily workloads. This approach allows the company to maintain the performance of the daily workloads while still being able to run

resource-intensive reports. Creating a backup and restoring it (Option B) is a more time-consuming process and does not provide the same level of performance as a read replica. Exporting data to Amazon S3 and using Athena (Option C) would require additional development and is not optimized for the workload described. Resizing the DB instance (Option D) may not be as cost-effective and would provide excess capacity for most of the month.

解析: Option A, creating a read replica of the database, is the most effective solution for maintaining performance during periodic heavy reporting workloads. The read replica can handle the additional query load, thus preventing a slowdown of the primary database that serves the daily workloads. This approach allows the company to maintain the performance of the daily workloads while still being able to run resource-intensive reports. Creating a backup and restoring it (Option B) is a more time-consuming process and does not provide the same level of performance as a read replica. Exporting data to Amazon S3 and using Athena (Option C) would require additional development and is not optimized for the workload described. Resizing the DB instance (Option D) may not be as cost-effective and would provide excess capacity for most of the month.

510. Question #591A 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**?
- 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.

答案: D

解析: Option D, using Amazon API Gateway, is the most cost-effective solution for routing incoming requests to the appropriate microservices in an Amazon EKS cluster. API Gateway is a fully managed service that can handle the routing of HTTP/S requests to the correct microservice endpoints, providing a scalable and efficient method for managing API traffic. This approach is more cost-effective than provisioning a Network Load Balancer (Option A) or an Application Load Balancer (Option B), which may involve additional costs and complexity. Using an AWS Lambda function (Option C) to manage the connection between requests and EKS is less efficient and would not be as scalable or cost-effective for this use case.

解析: Option D, using Amazon API Gateway, is the most cost-effective solution for routing incoming requests to the appropriate microservices in an Amazon EKS cluster. API Gateway is a fully managed service that can handle the routing of HTTP/S requests to the correct microservice endpoints, providing a scalable and efficient method for managing API traffic. This approach is more cost-effective than provisioning a Network Load Balancer (Option A) or an Application Load Balancer (Option B), which may involve additional costs and complexity. Using an AWS Lambda function (Option C) to manage the connection between requests and EKS is less efficient and would not be as scalable or cost-effective for this use case.

511. Question #592A 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?

- 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.

答案: D

解析: Option D, using Amazon S3 in conjunction with Amazon CloudFront and signed URLs, is the most cost-effective and scalable solution for distributing copyrighted images globally while restricting access to specific countries. CloudFront can be configured with geographic restrictions to deny access to users from certain countries, and signed URLs can be used to provide secure, time-limited access to content for individual customers. This approach minimizes costs by leveraging the global distribution and caching capabilities of CloudFront, reducing the need for public bucket access or IAM user management, and avoiding the operational overhead and potential scalability issues associated with running EC2 instances behind ALBs.

解析: Option D, using Amazon S3 in conjunction with Amazon CloudFront and signed URLs, is the most cost-effective and scalable solution for distributing copyrighted images globally while restricting access to specific countries. CloudFront can be configured with geographic restrictions to deny access to users from certain countries, and signed URLs can be used to provide secure, time-limited access to content for individual customers. This approach minimizes costs by leveraging the global distribution and caching capabilities of CloudFront, reducing the need for public bucket access or IAM user management, and avoiding the operational overhead and potential scalability issues associated with running EC2 instances behind ALBs.

512. Question #593A 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?

- 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.

答案：A

解析：Option A, using Multi-AZ Redis replication groups with shards containing multiple nodes, provides both high availability and data durability. Multi-AZ deployments offer automatic failover and data replication across multiple Availability Zones, ensuring that the Redis cluster remains available even if there is a failure in one AZ. This configuration also helps to maintain performance by spreading the workload across multiple nodes within a shard. While AOF (Option B) can enhance data persistence, it does not by itself provide the high availability across AZs. Option C's read replicas do not offer the same level of automatic failover and data replication as Multi-AZ replication groups. Auto Scaling (Option D) can help maintain performance during variable load but does not address cross-AZ replication or failover.

解析：Option A, using Multi-AZ Redis replication groups with shards containing multiple nodes, provides both high availability and data durability. Multi-AZ deployments offer automatic failover and data replication across multiple Availability Zones, ensuring that the Redis cluster remains available even if there is a failure in one AZ. This configuration also helps to maintain performance by spreading the workload across multiple nodes within a shard. While AOF (Option B) can enhance data persistence, it does not by itself provide the high availability across AZs. Option C's read replicas do not offer the same level of automatic failover and data replication as Multi-AZ replication

groups. Auto Scaling (Option D) can help maintain performance during variable load but does not address cross-AZ replication or failover.

513. Question #594A 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?

- 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.

答案: C

解析: Option C, using EC2 hibernation and Auto Scaling warm pools, is the solution that can reduce the launch time of the application. Hibernation allows instances to be stopped with their state saved, which can be quickly resumed, reducing the time to start from a stopped state compared to launching a new instance. Auto Scaling warm pools maintain a set of pre-initialized instances that can be quickly used to scale out, further reducing the time to launch instances. This approach is more cost-effective and efficient than maintaining multiple running instances (Option A), using Spot Instances (Option B) which may not be available or consistent, or using Capacity Reservations (Option D) which may not provide the same level of launch time reduction.

解析: Option C, using EC2 hibernation and Auto Scaling warm pools, is the solution that can reduce the launch time of the application. Hibernation allows instances to be stopped with their state saved, which can be quickly resumed, reducing the time to start from a stopped state compared to launching a new instance. Auto Scaling warm pools maintain a set of

pre-initialized instances that can be quickly used to scale out, further reducing the time to launch instances. This approach is more cost-effective and efficient than maintaining multiple running instances (Option A), using Spot Instances (Option B) which may not be available or consistent, or using Capacity Reservations (Option D) which may not provide the same level of launch time reduction.

514. Question #595A 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?

- 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.

答案：C

解析：Option C, using dynamic scaling, is the most cost-effective solution for handling sudden and unpredictable traffic increases. Dynamic scaling automatically adjusts the number of EC2 instances in the Auto Scaling group based on predefined metrics and thresholds, ensuring that the application can handle the increased load without manual intervention. This is more efficient than manual scaling (Option A), which requires human oversight, and more responsive than predictive scaling (Option B), which might not be as accurate for random traffic spikes. Schedule scaling (Option D) is not suitable for random traffic increases as it requires a predictable schedule.

解析：Option C, using dynamic scaling, is the most cost-effective solution for handling sudden and unpredictable traffic increases. Dynamic scaling automatically adjusts the number of EC2 instances in the Auto Scaling group based on predefined metrics and thresholds, ensuring that the application can handle the increased load without manual intervention. This is more efficient than manual scaling (Option A), which requires human oversight, and more responsive than predictive

scaling (Option B), which might not be as accurate for random traffic spikes. Schedule scaling (Option D) is not suitable for random traffic increases as it requires a predictable schedule.

515. Question #596 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?

- 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.

答案: A

解析: Option A, migrating the PostgreSQL database to Amazon Aurora Serverless v2, is the most cost-effective solution for handling unpredictable increases in database usage. Aurora Serverless v2 can automatically scale compute resources up and down based on the application's needs, which is ideal for unpredictable workloads like monthly sales events. This eliminates the need for manual intervention and the potential underutilization of resources. Enabling auto scaling on an EC2 instance (Option B) may not be as cost-effective due to the management overhead and the need for a larger instance type. Migrating to a larger RDS instance (Option C) would require provisioning additional capacity even during non-peak times. Migrating to Redshift (Option D) is not suitable for direct OLTP workloads typically associated with an ecommerce application.

解析: Option A, migrating the PostgreSQL database to Amazon Aurora Serverless v2, is the most cost-effective solution for handling

unpredictable increases in database usage. Aurora Serverless v2 can automatically scale compute resources up and down based on the application's needs, which is ideal for unpredictable workloads like monthly sales events. This eliminates the need for manual intervention and the potential underutilization of resources. Enabling auto scaling on an EC2 instance (Option B) may not be as cost-effective due to the management overhead and the need for a larger instance type. Migrating to a larger RDS instance (Option C) would require provisioning additional capacity even during non-peak times. Migrating to Redshift (Option D) is not suitable for direct OLTP workloads typically associated with an ecommerce application.

516. Question #597A 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?

- 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.

答案：B

解析：Option B, setting up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day, is the solution that will reduce latency. By pre-warming the application with provisioned concurrency, the application can quickly respond to the initial surge in requests, reducing cold start times and latency. This is more effective than simply increasing the throttling limit (Option A), which does not address the cold start issue. Creating a CloudWatch alarm (Option C) or increasing function memory (Option D) does not directly impact the latency caused by Lambda cold starts.

解析: Option B, setting up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day, is the solution that will reduce latency. By pre-warming the application with provisioned concurrency, the application can quickly respond to the initial surge in requests, reducing cold start times and latency. This is more effective than simply increasing the throttling limit (Option A), which does not address the cold start issue. Creating a CloudWatch alarm (Option C) or increasing function memory (Option D) does not directly impact the latency caused by Lambda cold starts.

517. Question #600A 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?

- 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.

答案: A

解析: Option A, deploying a Network Load Balancer (NLB), is the recommended solution. NLB is designed to handle millions of requests per second and is capable of managing high throughput at low latency, which meets the company's performance requirements. NLB operates at the connection level (Layer 4) and can distribute traffic across multiple targets using the required nonstandard TCP port. ALB (Option B) operates

at the application layer (Layer 7) and is more suited for HTTP/HTTPS traffic. CloudFront (Option C) is primarily used for content delivery and is not designed for generic TCP traffic. API Gateway (Option D) with Lambda (provisioned concurrency) would not be able to match the performance and scale required for 3 million requests per second.

解析：Option A, deploying a Network Load Balancer (NLB), is the recommended solution. NLB is designed to handle millions of requests per second and is capable of managing high throughput at low latency, which meets the company's performance requirements. NLB operates at the connection level (Layer 4) and can distribute traffic across multiple targets using the required nonstandard TCP port. ALB (Option B) operates at the application layer (Layer 7) and is more suited for HTTP/HTTPS traffic. CloudFront (Option C) is primarily used for content delivery and is not designed for generic TCP traffic. API Gateway (Option D) with Lambda (provisioned concurrency) would not be able to match the performance and scale required for 3 million requests per second.

518. Question #601A 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**?

- 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.

答案：B

解析：Option B, creating an Aurora read replica of the RDS for PostgreSQL DB instance and promoting it to a new Aurora PostgreSQL DB cluster, is the solution that will meet the requirements with the least operational overhead. This method allows for a smooth migration with minimal

downtime, as the read replica can be promoted to its own Aurora PostgreSQL DB cluster without significant service interruption. Creating a DB snapshot (Option A) or using pg_dump (Option D) would require more operational steps and potentially more downtime. Using data import from Amazon S3 (Option C) is not a supported method for migrating from RDS PostgreSQL to Aurora PostgreSQL. A(50%) B(50%)

解析: Option B, creating an Aurora read replica of the RDS for PostgreSQL DB instance and promoting it to a new Aurora PostgreSQL DB cluster, is the solution that will meet the requirements with the least operational overhead. This method allows for a smooth migration with minimal downtime, as the read replica can be promoted to its own Aurora PostgreSQL DB cluster without significant service interruption. Creating a DB snapshot (Option A) or using pg_dump (Option D) would require more operational steps and potentially more downtime. Using data import from Amazon S3 (Option C) is not a supported method for migrating from RDS PostgreSQL to Aurora PostgreSQL. A(50%) B(50%)

519. Question #602A 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?

- 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.

答案: C

解析: Option C, using AWS Backup to set up a backup plan for the entire group of EC2 instances, is the solution that requires the least amount of effort. AWS Backup is a fully managed service that can automate and centralize the backup process across multiple EBS volumes and EC2 instances. This approach eliminates the need for manual snapshot creation and the complexity of using CloudFormation templates or Elastic Beanstalk (Options A and B), as well as the need to develop and maintain custom Lambda functions (Option D). The AWS Backup API and CLI can further streamline the backup and restore process.

解析: Option C, using AWS Backup to set up a backup plan for the entire group of EC2 instances, is the solution that requires the least amount of effort. AWS Backup is a fully managed service that can automate and centralize the backup process across multiple EBS volumes and EC2 instances. This approach eliminates the need for manual snapshot creation and the complexity of using CloudFormation templates or Elastic Beanstalk (Options A and B), as well as the need to develop and maintain custom Lambda functions (Option D). The AWS Backup API and CLI can further streamline the backup and restore process.

520. Question #603A 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?

- 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.

答案：B

解析：Option B, using the AWS Step Functions Map state in Distributed mode, is the solution that offers the most operational efficiency for large-scale parallel processing of semistructured data stored in Amazon S3. The Map state in Distributed mode allows for the processing of large datasets in parallel by automatically managing the distribution and execution of tasks across multiple workers, scaling as needed without the need for manual intervention. This is more efficient than using Inline mode (Option A), which has limitations on the number of tasks that can be executed in parallel. While AWS Glue (Option C) and AWS Lambda (Option D) can also process data in parallel, they may require more complex setup and management compared to the serverless and fully managed nature of Step Functions with Distributed mode.

解析：Option B, using the AWS Step Functions Map state in Distributed mode, is the solution that offers the most operational efficiency for large-scale parallel processing of semistructured data stored in Amazon S3. The Map state in Distributed mode allows for the processing of large datasets in parallel by automatically managing the distribution and execution of tasks across multiple workers, scaling as needed without the need for manual intervention. This is more efficient than using Inline mode (Option A), which has limitations on the number of tasks that can be executed in parallel. While AWS Glue (Option C) and AWS Lambda (Option D) can also process data in parallel, they may require more complex setup and management compared to the serverless and fully managed nature of Step Functions with Distributed mode.

521. Question #604A 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?

- 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.

答案: D

解析: Option D, using multiple AWS Snowball devices, is the most viable solution for migrating 10 PB of data within the given time and bandwidth constraints. Given the large amount of data and the limited uplink bandwidth, transferring data over the internet using DataSync (Option A), rsync (Option B), or the AWS CLI (Option C) would be time-consuming and may not complete within the 6-week timeframe. Snowball devices are designed for such large data migrations, allowing for rapid data transfer through physical shipment and avoiding the bottleneck of internet bandwidth.

解析: Option D, using multiple AWS Snowball devices, is the most viable solution for migrating 10 PB of data within the given time and bandwidth constraints. Given the large amount of data and the limited uplink bandwidth, transferring data over the internet using DataSync (Option A), rsync (Option B), or the AWS CLI (Option C) would be time-consuming and may not complete within the 6-week timeframe. Snowball devices are designed for such large data migrations, allowing for rapid data transfer through physical shipment and avoiding the bottleneck of internet bandwidth.

522. Question #605A 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?

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.

答案: D

解析: Option D, deploying an AWS Storage Gateway volume gateway configured with cached volumes, is the solution that meets the requirements. This setup allows for low-latency access to frequently used data by storing it locally, while the less frequently accessed data is stored in Amazon S3. This reduces the need for on-premises storage servers and provides a seamless transition with minimal infrastructure changes. Amazon S3 File Gateway (Option A) is designed for file-level storage, not block storage like iSCSI. EBS storage with backups to Amazon S3 (Option B) does not provide the low-latency access required. Stored volumes (Option C) would store all data on-premises, which does not reduce the dependency on on-premises servers.

解析: Option D, deploying an AWS Storage Gateway volume gateway configured with cached volumes, is the solution that meets the requirements. This setup allows for low-latency access to frequently used data by storing it locally, while the less frequently accessed data is stored in Amazon S3. This reduces the need for on-premises storage servers and provides a seamless transition with minimal infrastructure changes. Amazon S3 File Gateway (Option A) is designed for file-level storage, not block storage like iSCSI. EBS storage with backups to Amazon S3 (Option B) does not provide the low-latency access required. Stored volumes (Option C) would store all data on-premises, which does not reduce the dependency on on-premises servers.

523. Question #606A 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?

- 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.

答案：B

解析：Option B, storing objects in S3 Standard and transitioning them to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, is the most cost-effective solution. This approach ensures high durability and availability during the initial 30 days when access is frequent, and then transitions the objects to a lower-cost storage class for long-term storage with reduced access frequency. S3 Glacier (Option A) is designed for long-term archiving and not ideal for objects that may still be accessed, albeit less frequently. S3 One Zone-IA (Option C) is similar to S3 Standard-IA but with reduced redundancy and higher risk of data loss, making it less suitable for maximizing durability. S3 Intelligent-Tiering (Option D) automatically moves objects between access tiers based on access patterns, which could be more costly and complex than necessary for the described use case.

解析：Option B, storing objects in S3 Standard and transitioning them to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, is the most cost-effective solution. This approach ensures high durability and availability during the initial 30 days when access is frequent, and then transitions the objects to a lower-cost storage class for long-term storage with reduced access frequency. S3 Glacier (Option A) is designed for long-term archiving and not ideal for objects that may still be

accessed, albeit less frequently. S3 One Zone-IA (Option C) is similar to S3 Standard-IA but with reduced redundancy and higher risk of data loss, making it less suitable for maximizing durability. S3 Intelligent-Tiering (Option D) automatically moves objects between access tiers based on access patterns, which could be more costly and complex than necessary for the described use case.

524. Question #607A 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?

- 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.

答案: C

解析: Option C, creating an Amazon S3 bucket and updating the application to store documents there while keeping the metadata in the RDS database, is the most cost-effective solution. This approach offloads the storage of large blobs from the RDS instance to S3, which is optimized for storing large amounts of data. By storing only metadata in the database, the performance is improved, and costs are reduced since S3 is more cost-effective for storing large blobs than using General Purpose SSD EBS

volumes for a database. Additionally, S3 provides high availability and durability. Options A and B involve resizing and type changing of EBS storage, which may not be as cost-effective and still does not address the performance issues with large blobs. Option D is not cost-effective because DynamoDB is not optimized for storing large blobs, and migrating data from Oracle to DynamoDB would be complex and unnecessary for this use case.

解析: Option C, creating an Amazon S3 bucket and updating the application to store documents there while keeping the metadata in the RDS database, is the most cost-effective solution. This approach offloads the storage of large blobs from the RDS instance to S3, which is optimized for storing large amounts of data. By storing only metadata in the database, the performance is improved, and costs are reduced since S3 is more cost-effective for storing large blobs than using General Purpose SSD EBS volumes for a database. Additionally, S3 provides high availability and durability. Options A and B involve resizing and type changing of EBS storage, which may not be as cost-effective and still does not address the performance issues with large blobs. Option D is not cost-effective because DynamoDB is not optimized for storing large blobs, and migrating data from Oracle to DynamoDB would be complex and unnecessary for this use case.

525. Question #608A 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 increasing 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?

- 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.

答案：A

解析：Option A, associating an AWS WAF web ACL with the ALB and using IP rule sets to filter traffic, is the most effective solution for restricting access to a known set of IP addresses. This approach allows for the registration of IP addresses and provides a centralized way to manage and update the list of allowed IPs. AWS WAF is designed to filter malicious traffic and can be configured to allow or deny traffic from specific IP addresses. Option B, using AWS Firewall Manager, could also be used to manage WAF rules but is not necessary and adds an additional layer of management. Option C, using a Lambda function for authorization, would introduce unnecessary complexity and potential latency. Option D, configuring network ACLs, would not be as efficient since network ACLs are stateless and would require rules for each IP address, which is not scalable for 20,000 locations.

解析：Option A, associating an AWS WAF web ACL with the ALB and using IP rule sets to filter traffic, is the most effective solution for restricting access to a known set of IP addresses. This approach allows for the registration of IP addresses and provides a centralized way to manage and update the list of allowed IPs. AWS WAF is designed to filter malicious traffic and can be configured to allow or deny traffic from specific IP addresses. Option B, using AWS Firewall Manager, could also be used to manage WAF rules but is not necessary and adds an additional

layer of management. Option C, using a Lambda function for authorization, would introduce unnecessary complexity and potential latency. Option D, configuring network ACLs, would not be as efficient since network ACLs are stateless and would require rules for each IP address, which is not scalable for 20,000 locations.

526. Question #609A 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?**

- 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.

答案：B

解析：Option B, creating data filters to implement row-level and cell-level security, is the solution that meets the requirements with the least operational overhead. Lake Formation supports data filters that can restrict access to specific rows and cells based on the values in those rows and cells. This allows for fine-grained access control without the need for custom code or periodic queries. Option A, using IAM roles, provides only a coarse level of access control. Options C and D, involving AWS Lambda functions, would require ongoing maintenance and are not as efficient for the task as the native data filter functionality of Lake Formation.

解析：Option B, creating data filters to implement row-level and cell-level security, is the solution that meets the requirements with the least operational overhead. Lake Formation supports data filters that can

restrict access to specific rows and cells based on the values in those rows and cells. This allows for fine-grained access control without the need for custom code or periodic queries. Option A, using IAM roles, provides only a coarse level of access control. Options C and D, involving AWS Lambda functions, would require ongoing maintenance and are not as efficient for the task as the native data filter functionality of Lake Formation.

527. Question #610A 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?

- 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.

答案：B

解析：Option B, deploying a gateway VPC endpoint for Amazon S3 and setting up an AWS Direct Connect connection, is the solution that meets the requirements. A gateway VPC endpoint for S3 allows for private connectivity between the VPC and S3 without data traversing the public internet, thus complying with the laws. Direct Connect establishes a dedicated network connection from the on-premises data center to the VPC, ensuring secure and private access to the EC2 instances. Option A, using an interface VPC endpoint and a Site-to-Site VPN, does not provide the

necessary private connectivity to S3. Option C, using AWS Transit Gateway, is not required for this scenario and adds unnecessary complexity. Option D, setting up proxy EC2 instances, would not meet the requirement of not transmitting data over the public internet.

解析: Option B, deploying a gateway VPC endpoint for Amazon S3 and setting up an AWS Direct Connect connection, is the solution that meets the requirements. A gateway VPC endpoint for S3 allows for private connectivity between the VPC and S3 without data traversing the public internet, thus complying with the laws. Direct Connect establishes a dedicated network connection from the on-premises data center to the VPC, ensuring secure and private access to the EC2 instances. Option A, using an interface VPC endpoint and a Site-to-Site VPN, does not provide the necessary private connectivity to S3. Option C, using AWS Transit Gateway, is not required for this scenario and adds unnecessary complexity. Option D, setting up proxy EC2 instances, would not meet the requirement of not transmitting data over the public internet.

528. Question #611A 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?

- 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.

答案：A

解析：Option A, using Amazon Kinesis Data Streams and AWS Lambda, is the recommended solution for scalability. Kinesis Data Streams can handle large amounts of streaming data, scaling automatically to accommodate data volume spikes. AWS Lambda can process the incoming data in a serverless manner, ensuring that there is no limit to the compute capacity based on the number of EC2 instances. This approach will alleviate the 503 errors by providing the necessary scalability. Option B, using API Gateway with a usage plan, does not address the scalability of data processing. Option C, using SNS, is not designed for large-scale data ingestion. Option D, repackaging the application as a container and using ECS with EC2 launch type, still relies on the scaling capabilities of the underlying EC2 instances and does not inherently solve the scalability issue.

解析：Option A, using Amazon Kinesis Data Streams and AWS Lambda, is the recommended solution for scalability. Kinesis Data Streams can handle large amounts of streaming data, scaling automatically to accommodate data volume spikes. AWS Lambda can process the incoming data in a serverless manner, ensuring that there is no limit to the compute capacity based on the number of EC2 instances. This approach will alleviate the 503 errors by providing the necessary scalability. Option B, using API Gateway with a usage plan, does not address the scalability of data processing. Option C, using SNS, is not designed for large-scale data ingestion. Option D, repackaging the application as a container and using ECS with EC2 launch type, still relies on the scaling capabilities of the underlying EC2 instances and does not inherently solve the scalability issue.

529. Question #612A 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?

- 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.

答案：D

解析：Option D, configuring a VPC endpoint for Amazon S3, is the solution that meets the requirements. A VPC endpoint provides private connectivity between the VPC and S3 without the need for an internet gateway, NAT device, or VPN connection. This ensures that the application can access the S3 bucket without using the public internet, maintaining the privacy and security of sensitive information. Options A, B, and C would all require the use of the public internet or a VPN, which does not meet the specified requirements.

解析：Option D, configuring a VPC endpoint for Amazon S3, is the solution that meets the requirements. A VPC endpoint provides private connectivity between the VPC and S3 without the need for an internet gateway, NAT device, or VPN connection. This ensures that the application can access the S3 bucket without using the public internet, maintaining the privacy and security of sensitive information. Options A, B, and C would all require the use of the public internet or a VPN, which does not meet the specified requirements.

530. Question #613A 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?

- 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).

答案：B

解析：Option B, enabling secrets encryption in the EKS cluster using AWS KMS, is the solution that meets the requirements with the least operational overhead. EKS supports encrypting Kubernetes secrets at the cluster level with AWS KMS, providing an automated way to encrypt secrets without the need for additional development effort or operational complexity. Option A would require changes to the container application, and Option C would necessitate the implementation and management of a Lambda function. Option D, while it could store encrypted parameters, does not natively integrate with EKS to encrypt Kubernetes secrets.

解析：Option B, enabling secrets encryption in the EKS cluster using AWS KMS, is the solution that meets the requirements with the least operational overhead. EKS supports encrypting Kubernetes secrets at the cluster level with AWS KMS, providing an automated way to encrypt secrets without the need for additional development effort or operational complexity. Option A would require changes to the container application, and Option C would necessitate the implementation and management of a Lambda function. Option D, while it could store encrypted parameters, does not natively integrate with EKS to encrypt Kubernetes secrets.

531. Question #614A 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?

- 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.

答案: D

解析: Option D, deploying an Application Load Balancer (ALB) with a target group for the application servers and configuring the security group to allow access only from the web servers, is the solution that meets the requirements. ALB can route traffic to the application servers and, through security group configurations, restrict access to only the necessary entities, in this case, the web servers. This provides an application-level load balancing solution with fine-grained access control. Options A and B do not provide the necessary access control at the application server level, and Option C, while using a Network Load Balancer (NLB) could distribute traffic, does not integrate with security groups in the same way as an ALB does for access control purposes.

解析: Option D, deploying an Application Load Balancer (ALB) with a target group for the application servers and configuring the security group to allow access only from the web servers, is the solution that meets the requirements. ALB can route traffic to the application servers and, through security group configurations, restrict access to only the necessary entities, in this case, the web servers. This provides an application-level load balancing solution with fine-grained access

control. Options A and B do not provide the necessary access control at the application server level, and Option C, while using a Network Load Balancer (NLB) could distribute traffic, does not integrate with security groups in the same way as an ALB does for access control purposes.

532. Question #615A 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?

- 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.

答案: D

解析: Option D, configuring Amazon CloudWatch Container Insights in the existing EKS cluster, is the solution that meets the requirements.

CloudWatch Container Insights can collect, aggregate, and summarize metrics and logs from the containers running in the EKS cluster, providing a centralized view in the CloudWatch console. This is a native AWS service designed for container monitoring and does not require additional setup for capturing data events like CloudTrail (Option C) or using a service mesh like App Mesh (Option B). **Running the CloudWatch agent (Option A) is part of the process, but Container Insights is the feature that provides the required insights and centralized view.**

解析: Option D, configuring Amazon CloudWatch Container Insights in the existing EKS cluster, is the solution that meets the requirements.

CloudWatch Container Insights can collect, aggregate, and summarize metrics and logs from the containers running in the EKS cluster,

providing a centralized view in the CloudWatch console. This is a native AWS service designed for container monitoring and does not require additional setup for capturing data events like CloudTrail (Option C) or using a service mesh like App Mesh (Option B). Running the CloudWatch agent (Option A) is part of the process, but Container Insights is the feature that provides the required insights and centralized view.

533. Question #616A 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?

- 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.

答案: C

解析: Option C, configuring Amazon GuardDuty to monitor and report findings to AWS Security Hub, is the solution that meets the requirements. GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior in AWS accounts and workloads. It can integrate with AWS Security Hub, which provides a comprehensive view of security alerts and findings, including those related to S3 bucket access. This allows for centralized monitoring, alerting, and response to suspicious activities. Amazon Macie (Option A) focuses on data security and does not provide the same breadth of threat detection. Amazon Inspector (Option B) is for vulnerability assessment and does not monitor access patterns to S3. AWS Config (Option D)

monitors configuration changes and compliance but does not detect threats.

解析: Option C, configuring Amazon GuardDuty to monitor and report findings to AWS Security Hub, is the solution that meets the requirements. GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior in AWS accounts and workloads. It can integrate with AWS Security Hub, which provides a comprehensive view of security alerts and findings, including those related to S3 bucket access. This allows for centralized monitoring, alerting, and response to suspicious activities. Amazon Macie (Option A) focuses on data security and does not provide the same breadth of threat detection. Amazon Inspector (Option B) is for vulnerability assessment and does not monitor access patterns to S3. AWS Config (Option D) monitors configuration changes and compliance but does not detect threats.

534. Question #618A 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?

- A. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- B. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

- C. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- D. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ 2 deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

答案：C

解析：Option C is the correct solution. A Multi-AZ deployment type for the FSx for Windows File Server file system in us-east-1 ensures high availability and meets the RPO of 5 minutes. Using AWS Backup to create a daily backup plan that includes a backup rule to copy the backup to us-west-2 provides the replication needed across regions. Configuring AWS Backup Vault Lock in compliance mode ensures that the backups cannot be deleted for the specified duration of 5 years, aligning with the company's requirements.

解析：Option C is the correct solution. A Multi-AZ deployment type for the FSx for Windows File Server file system in us-east-1 ensures high availability and meets the RPO of 5 minutes. Using AWS Backup to create a daily backup plan that includes a backup rule to copy the backup to us-west-2 provides the replication needed across regions. Configuring AWS Backup Vault Lock in compliance mode ensures that the backups cannot be deleted for the specified duration of 5 years, aligning with the company's requirements.

535. Question #619A 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?

- 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 Amazon Resource Name (ARN) in the management account.

答案：C

解析：Option C, creating a service control policy (SCP) that prohibits changes to CloudTrail and attaching it to the developer accounts, is the action that meets the requirements. SCPs are used in AWS Organizations to set permissions boundaries for accounts, ensuring that developers cannot modify the CloudTrail configuration. This is a more effective approach than creating IAM policies (Option A), which can be bypassed by root users, or creating a new trail (Option B), which does not prevent modification of existing trails. Option D, creating a service-linked role, does not address the prevention of modifications to CloudTrail configurations.

解析：Option C, creating a service control policy (SCP) that prohibits changes to CloudTrail and attaching it to the developer accounts, is the action that meets the requirements. SCPs are used in AWS Organizations to set permissions boundaries for accounts, ensuring that developers cannot modify the CloudTrail configuration. This is a more effective approach than creating IAM policies (Option A), which can be bypassed by root users, or creating a new trail (Option B), which does not prevent modification of existing trails. Option D, creating a service-linked role, does not address the prevention of modifications to CloudTrail configurations.

536. Question #620A 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?

- 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

答案: C

解析: Option C, a Provisioned IOPS SSD Amazon EBS volume, is the recommended storage type for business-critical applications requiring durable storage and consistent, low latency performance. Provisioned IOPS SSD volumes are designed to deliver high-performance, consistent I/O and are well-suited for critical workloads. Instance store volumes (Option A) are attached directly to the instance and are not durable as they are not preserved if the instance restarts. Amazon ElastiCache for Memcached (Option B) is an in-memory data store and not a persistent storage solution. Throughput Optimized HDD EBS volumes (Option D) are designed for high-throughput workloads and are not optimized for low latency.

解析: Option C, a Provisioned IOPS SSD Amazon EBS volume, is the recommended storage type for business-critical applications requiring durable storage and consistent, low latency performance. Provisioned IOPS SSD volumes are designed to deliver high-performance, consistent I/O and are well-suited for critical workloads. Instance store volumes (Option A) are attached directly to the instance and are not durable as they are not preserved if the instance restarts. Amazon ElastiCache for Memcached (Option B) is an in-memory data store and not a persistent storage solution. Throughput Optimized HDD EBS volumes (Option D) are designed for high-throughput workloads and are not optimized for low latency.

537. Question #621An 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?**

- 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.

答案：A

解析：Option A, using S3 Cross-Region Replication, is the solution that meets the requirement with the least operational effort. Cross-Region Replication is a built-in feature of S3 that automatically replicates new objects added to the source bucket to a destination bucket in a different region, requiring no additional configuration or manual intervention.

Option B, setting up CORS, does not replicate objects. Option C, using S3 Lifecycle rules, and Option D, using S3 event notifications with Lambda, would both require additional setup and custom logic to replicate objects, which is not as efficient or low-effort as using Cross-Region Replication.

解析：Option A, using S3 Cross-Region Replication, is the solution that meets the requirement with the least operational effort. Cross-Region Replication is a built-in feature of S3 that automatically replicates new objects added to the source bucket to a destination bucket in a different region, requiring no additional configuration or manual intervention.

Option B, setting up CORS, does not replicate objects. Option C, using S3 Lifecycle rules, and Option D, using S3 event notifications with Lambda, would both require additional setup and custom logic to replicate objects, which is not as efficient or low-effort as using Cross-Region

Replication.

538. Question #623A 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?

- 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.

答案: B

解析: Correct Answer: B waiting

解析: Correct Answer: B waiting

539. Question #624A 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?

- 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.

答案: D

解析: Option D, configuring SAML 2.0-based federation, allows the company to use their existing Active Directory identities to access AWS resources without creating and managing separate IAM users. This approach streamlines identity management and provides a seamless experience for users, as they can use their on-premises credentials to access both local and AWS-based resources.

解析: Option D, configuring SAML 2.0-based federation, allows the company to use their existing Active Directory identities to access AWS resources without creating and managing separate IAM users. This approach streamlines identity management and provides a seamless experience for users, as they can use their on-premises credentials to access both local and AWS-based resources.

540. Question #625A 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?

- 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

答案: C

解析: Option C, configuring Amazon Route 53 with a geolocation policy, is the appropriate choice for ensuring that users are served the correct content based on their geographic location. This allows the company to route users to the appropriate distribution point that has the legal rights to display the content, thereby adhering to distribution rights.

解析: Option C, configuring Amazon Route 53 with a geolocation policy, is the appropriate choice for ensuring that users are served the correct content based on their geographic location. This allows the company to route users to the appropriate distribution point that has the legal rights to display the content, thereby adhering to distribution rights.

541. Question #626A 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?

- 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.

答案：B

解析：Option B, deploying an AWS DataSync agent, is the solution that will meet the requirements. DataSync is designed to automate data transfer between on-premises storage and AWS services like S3, and it includes data integrity checks to ensure the data has been transferred correctly.

解析：Option B, deploying an AWS DataSync agent, is the solution that will meet the requirements. DataSync is designed to automate data transfer between on-premises storage and AWS services like S3, and it includes data integrity checks to ensure the data has been transferred correctly.

542. Question #627A 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?

- 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 tiles. Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- C. Migrate the servers to AWS by using AWS Server Migration Service (AWS SMS). Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- D. Launch an Amazon EC2 instance in an Auto Scaling group across two Availability Zones. Import zone files. Set the desired capacity to 1 and the maximum capacity to 3 for the Auto Scaling group. Configure scaling alarms to scale based on CPU utilization.

答案：A

解析：Option A, creating new hosted zones in Amazon Route 53, is the recommended solution. Route 53 is a highly available and scalable cloud DNS web service that can easily handle the load of 200 zones and 1 million requests per day. By using Route 53, the company can eliminate the operational overhead of managing DNS servers and ensure high availability without the need for Auto Scaling or additional monitoring with CloudWatch.

解析：Option A, creating new hosted zones in Amazon Route 53, is the recommended solution. Route 53 is a highly available and scalable cloud DNS web service that can easily handle the load of 200 zones and 1 million requests per day. By using Route 53, the company can eliminate the operational overhead of managing DNS servers and ensure high availability without the need for Auto Scaling or additional monitoring with CloudWatch.

543. Question #628A 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?

- 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.

答案: C

解析: Option C, configuring S3 Storage Lens, is the solution that meets the requirements with the least operational overhead. S3 Storage Lens provides insights into the usage of S3 resources across multiple accounts and can generate metrics on incomplete multipart uploads, which can be used for cost compliance reporting. This solution does not require additional configuration of AWS Config rules or service control policies, and it is more focused on S3 usage than creating a Multi-Region Access Point, which is not primarily designed for reporting purposes.

解析: Option C, configuring S3 Storage Lens, is the solution that meets the requirements with the least operational overhead. S3 Storage Lens provides insights into the usage of S3 resources across multiple accounts and can generate metrics on incomplete multipart uploads, which can be used for cost compliance reporting. This solution does not require additional configuration of AWS Config rules or service control policies, and it is more focused on S3 usage than creating a Multi-Region Access Point, which is not primarily designed for reporting purposes.

544. Question #629A 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?

- 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.**

答案: D

解析: Option D, using Amazon RDS Blue/Green Deployments, is the solution that meets the requirements with the least operational overhead.

Blue/Green deployments allow the company to upgrade the database version with minimal downtime by creating a new environment and promoting it to production once ready. This approach ensures that the production database remains available during the upgrade process and allows for testing in the new environment before switching over.

解析: Option D, using Amazon RDS Blue/Green Deployments, is the solution that meets the requirements with the least operational overhead.

Blue/Green deployments allow the company to upgrade the database version with minimal downtime by creating a new environment and promoting it to production once ready. This approach ensures that the production database remains available during the upgrade process and allows for testing in the new environment before switching over.

545. Question #630A 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?

- 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.

答案：C

解析：Option C, using an Amazon ECS Fargate task, is the most cost-effective solution for a data processing job that runs once daily for up to 2 hours. Fargate is a serverless offering for Amazon ECS that allows users to run containers without managing the underlying infrastructure. It scales the resources automatically, and users are charged based on the actual usage. This eliminates the need for a Reserved Instance (Option A) and provides a more cost-effective and efficient way to run containerized workloads compared to managing an EC2 instance (Option D) or using Lambda (Option B), which has a maximum execution time limit that might not suffice for a 2-hour job.

解析：Option C, using an Amazon ECS Fargate task, is the most cost-effective solution for a data processing job that runs once daily for up to 2 hours. Fargate is a serverless offering for Amazon ECS that allows users to run containers without managing the underlying infrastructure. It scales the resources automatically, and users are charged based on the actual usage. This eliminates the need for a Reserved Instance (Option A) and provides a more cost-effective and efficient way to run containerized workloads compared to managing an EC2 instance (Option D) or using Lambda (Option B), which has a maximum execution time limit that might not suffice for a 2-hour job.

546. Question #631A 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?

- A. Use Amazon Neptune to store the information. Use Amazon Kinesis Data Streams to process changes in the database.
- B. Use Amazon Neptune to store the information. Use Neptune Streams to process changes in the database.
- C. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Amazon Kinesis Data Streams to process changes in the

database.

- D. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Neptune Streams to process changes in the database.

答案：B

解析：Option B, using Amazon Neptune with Neptune Streams, is the solution that meets the requirements with the least operational overhead.

Amazon Neptune is a graph database designed to store and process highly connected data, making it suitable for social media applications with complex relationships. Neptune Streams captures a time-ordered sequence of data changes, which can be used to monitor and analyze changes in the database, providing insights and recommendations to users.

解析：Option B, using Amazon Neptune with Neptune Streams, is the solution that meets the requirements with the least operational overhead. Amazon Neptune is a graph database designed to store and process highly connected data, making it suitable for social media applications with complex relationships. Neptune Streams captures a time-ordered sequence of data changes, which can be used to monitor and analyze changes in the database, providing insights and recommendations to users.

547. Question #632A 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?

- A. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- 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.

答案：C

解析: Option C, storing the data in Amazon EFS, is the recommended solution. Amazon EFS is a scalable file storage service for use with AWS Cloud services and on-premises resources. It provides the ability to mount the same file system across multiple EC2 instances and Availability Zones, making it ideal for applications that require shared access to data. This eliminates the need for individual EBS volumes (Option B) or a shared EBS volume with Provisioned IOPS (Option D), which are not designed for shared access and can have limitations in terms of scalability and performance. S3 Glacier (Option A) is not suitable for this use case due to its retrieval times and is more appropriate for long-term archival storage.

解析: Option C, storing the data in Amazon EFS, is the recommended solution. Amazon EFS is a scalable file storage service for use with AWS Cloud services and on-premises resources. It provides the ability to mount the same file system across multiple EC2 instances and Availability Zones, making it ideal for applications that require shared access to data. This eliminates the need for individual EBS volumes (Option B) or a shared EBS volume with Provisioned IOPS (Option D), which are not designed for shared access and can have limitations in terms of scalability and performance. S3 Glacier (Option A) is not suitable for this use case due to its retrieval times and is more appropriate for long-term archival storage.

548. Question #633A 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?
- 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.

答案: C

解析: Option C, creating a read replica from the source DB instance and serving read traffic from the read replica, is the correct action to improve performance. By offloading read queries to the read replica, the primary instance can focus on write operations, which are not supported by the standby replica in a Multi-AZ deployment. This distribution of read and write operations can significantly improve the overall performance of the application.

解析: Option C, creating a read replica from the source DB instance and serving read traffic from the read replica, is the correct action to improve performance. By offloading read queries to the read replica, the primary instance can focus on write operations, which are not supported by the standby replica in a Multi-AZ deployment. This distribution of read and write operations can significantly improve the overall performance of the application.

549. Question #634A 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?

- 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.

答案: C

解析: Option C, configuring cross-account access for the S3 bucket, is the solution that meets the requirements for security and operational efficiency. This allows the company to maintain control over the data

while granting specific agencies access to the S3 bucket they require. This approach avoids the security risks of making the bucket public (Option B) and the administrative overhead of managing individual IAM users (Option D). S3 global tables (Option A) are not designed for this use case and are more relevant for applications requiring high availability and consistency of data across multiple regions.

解析: Option C, configuring cross-account access for the S3 bucket, is the solution that meets the requirements for security and operational efficiency. This allows the company to maintain control over the data while granting specific agencies access to the S3 bucket they require. This approach avoids the security risks of making the bucket public (Option B) and the administrative overhead of managing individual IAM users (Option D). S3 global tables (Option A) are not designed for this use case and are more relevant for applications requiring high availability and consistency of data across multiple regions.

550. Question #635A 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?

- A. Create an AWS Lambda function to copy the data to an Amazon 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 the volumes to the secondary Region. Create a new FSx for ONTAP instance from the backup.
- C. Create an FSx for ONTAP instance in the secondary Region. Use NetApp SnapMirror to replicate data from the primary Region to the secondary Region.
- D. Create an Amazon Elastic File System (Amazon EFS) volume. Migrate the current data to the volume. Replicate the volume to the secondary Region.

答案: C

解析: Option C, creating an FSx for ONTAP instance in the secondary Region and using NetApp SnapMirror to replicate data, is the solution that meets the requirements with the least operational overhead.

SnapMirror is a replication technology specifically designed for disaster recovery and provides a way to replicate data between ONTAP file systems, including across different AWS Regions. This solution allows for the use of the same protocols in the secondary Region as in the primary Region, ensuring minimal changes to the operational workflows.

解析: Option C, creating an FSx for ONTAP instance in the secondary Region and using NetApp SnapMirror to replicate data, is the solution that meets the requirements with the least operational overhead.

SnapMirror is a replication technology specifically designed for disaster recovery and provides a way to replicate data between ONTAP file systems, including across different AWS Regions. This solution allows for the use of the same protocols in the secondary Region as in the primary Region, ensuring minimal changes to the operational workflows.

551. Question #636A 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 Simple Notification Service (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?

- A. Create an SNS subscription that processes the event in Amazon Elastic Container Service (Amazon ECS) before the event runs in Lambda.
- B. Create an SNS subscription that processes the event in Amazon Elastic Kubernetes Service (Amazon EKS) before the event runs in Lambda.
- C. Create an SNS subscription that sends the event to Amazon Simple Queue Service (Amazon SQS). Configure the SQS queue to trigger a Lambda function.**
- D. Create an SNS subscription that sends the event to AWS Server Migration Service (AWS SMS). Configure the Lambda function to poll from the SMS event.

答案: C

解析: Option C, creating an SNS subscription that sends the event to Amazon SQS and configuring the SQS queue to trigger a Lambda function, is the scalable solution for processing events from Amazon S3. This setup allows for the decoupling of event generation and processing, enabling the system to handle variable loads efficiently. SQS acts as a buffer that can store messages even when the processing system is overwhelmed, ensuring that no events are lost. Triggering a Lambda function from SQS provides a serverless approach to process the events, scaling automatically with the number of messages in the queue.

解析: Option C, creating an SNS subscription that sends the event to Amazon SQS and configuring the SQS queue to trigger a Lambda function, is the scalable solution for processing events from Amazon S3. This setup allows for the decoupling of event generation and processing, enabling the system to handle variable loads efficiently. SQS acts as a buffer that can store messages even when the processing system is overwhelmed, ensuring that no events are lost. Triggering a Lambda function from SQS provides a serverless approach to process the events, scaling automatically with the number of messages in the queue.

552. Question #638A 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?

- 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.

答案：A

解析：Option A, using an AWS Lambda function to create S3 presigned URLs, is the solution that meets the requirements with minimal operational overhead. This approach allows for secure, temporary access to S3 objects without the need to manage long-term credentials or IAM users for each employee. Presigned URLs can be generated dynamically and shared with employees as needed, providing a scalable and secure way to share data.

解析：Option A, using an AWS Lambda function to create S3 presigned URLs, is the solution that meets the requirements with minimal operational overhead. This approach allows for secure, temporary access to S3 objects without the need to manage long-term credentials or IAM users for each employee. Presigned URLs can be generated dynamically and shared with employees as needed, providing a scalable and secure way to share data.

553. Question #639A 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?

- 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

答案：A

解析：Option A, disabling session affinity (sticky sessions) on the ALB, is the correct action to resolve the issue of uneven traffic distribution. Sticky sessions can cause an imbalance in the load distribution if not configured properly. By disabling sticky sessions, the ALB is able to distribute incoming requests more evenly across all

EC2 instances, which can help to eliminate latency issues resulting from one instance receiving too much traffic.

解析: Option A, disabling session affinity (sticky sessions) on the ALB, is the correct action to resolve the issue of uneven traffic distribution. Sticky sessions can cause an imbalance in the load distribution if not configured properly. By disabling sticky sessions, the ALB is able to distribute incoming requests more evenly across all EC2 instances, which can help to eliminate latency issues resulting from one instance receiving too much traffic.

554. Question #641A 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?

- 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.

答案: B

解析: Option B, enabling Cost and Usage Reports in the management account and delivering the reports to Amazon S3 with subsequent analysis using Amazon Athena, is the most scalable and cost-effective solution. This approach allows for the storage of historical cost and usage data in S3, which is a highly durable and cost-effective storage solution. Athena can then be used to perform serverless, ad-hoc queries against this data, making it a scalable and efficient method for analyzing large volumes of data without the need for complex setup or high ongoing costs.

解析: Option B, enabling Cost and Usage Reports in the management account and delivering the reports to Amazon S3 with subsequent analysis using Amazon Athena, is the most scalable and cost-effective solution. This approach allows for the storage of historical cost and usage data in S3, which is a highly durable and cost-effective storage solution. Athena can then be used to perform serverless, ad-hoc queries against this data, making it a scalable and efficient method for analyzing large volumes of data without the need for complex setup or high ongoing costs.

555. Question #642A 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?

- 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.

答案: A

解析: Option A, attaching a Network Load Balancer (NLB) to the Auto Scaling group, is the correct solution for a gaming application that uses UDP packets. NLB can handle millions of requests per second and is capable of managing the high throughput and low latency required for gaming applications. It also scales in and out automatically with the Auto Scaling group, ensuring that the application can adapt to changes in traffic.

解析: Option A, attaching a Network Load Balancer (NLB) to the Auto Scaling group, is the correct solution for a gaming application that uses UDP packets. NLB can handle millions of requests per second and is capable of managing the high throughput and low latency required for gaming applications. It also scales in and out automatically with the

Auto Scaling group, ensuring that the application can adapt to changes in traffic.

556. Question #643A 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?

- 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.

答案: A

解析: Option A, storing the logs in Amazon S3 and using Amazon Athena for analysis, is the most cost-effective solution. Amazon S3 is a highly scalable and durable storage solution, and Athena allows for the execution of SQL-like queries directly against the data stored in S3. This serverless approach eliminates the need for the ongoing management and cost associated with maintaining a database or a cluster, making it a cost-effective choice for infrequent, on-demand analysis.

解析: Option A, storing the logs in Amazon S3 and using Amazon Athena for analysis, is the most cost-effective solution. Amazon S3 is a highly scalable and durable storage solution, and Athena allows for the execution of SQL-like queries directly against the data stored in S3. This serverless approach eliminates the need for the ongoing management and cost associated with maintaining a database or a cluster, making it a cost-effective choice for infrequent, on-demand analysis.

557. Question #645A 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?

- 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 Key Management Service (AWS KMS) managed key store.
- D. Use a custom key store backed by an AWS CloudHSM cluster.

答案：B

解析：Option B, using an AWS KMS external key store backed by an external key manager, allows the company to manage encryption and decryption with keys that are retained outside of the AWS Cloud. This solution meets the requirement of supporting a variety of external key managers and is the least operationally intensive option since it leverages the existing on-premises key manager.

解析：Option B, using an AWS KMS external key store backed by an external key manager, allows the company to manage encryption and decryption with keys that are retained outside of the AWS Cloud. This solution meets the requirement of supporting a variety of external key managers and is the least operationally intensive option since it leverages the existing on-premises key manager.

558. Question #646A 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?

- 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 for processing and postprocessing.

答案：C

解析：Option C, Amazon FSx for Lustre, is a high-performance file system designed for HPC workloads. It provides the required sub-millisecond latency and supports parallel access to a shared file system by multiple EC2 instances. Additionally, it can be linked to an S3 bucket for **postprocessing**, which meets the requirement for engineers to access the dataset after processing.

解析：Option C, Amazon FSx for Lustre, is a high-performance file system designed for HPC workloads. It provides the required sub-millisecond latency and supports parallel access to a shared file system by multiple EC2 instances. Additionally, it can be linked to an S3 bucket for postprocessing, which meets the requirement for engineers to access the dataset after processing.

559. Question #647A **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?

- 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.

答案：A

解析：Option A, AWS Global Accelerator, is designed to improve the availability and performance of applications by directing traffic to the optimal regional endpoint based on health and routing policies. It provides static IP addresses and supports both TCP and UDP traffic, making it suitable for Voice over IP applications. This solution allows for automated failover across AWS Regions and helps minimize latency without relying on IP address caching.

解析：Option A, AWS Global Accelerator, is designed to improve the availability and performance of applications by directing traffic to the optimal regional endpoint based on health and routing policies. It provides static IP addresses and supports both TCP and UDP traffic, making it suitable for Voice over IP applications. This solution allows for automated failover across AWS Regions and helps minimize latency without relying on IP address caching.

560. Question #648A 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?

- 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.

答案：B

解析: Option B, Amazon FSx for Lustre persistent file systems, is a high-performance file system that is designed for HPC workloads requiring rapid access to large datasets. The persistent file system maintains data even after reboots, which is necessary for a weather forecasting company that needs to process large amounts of data with high throughput and low latency.

解析: Option B, Amazon FSx for Lustre persistent file systems, is a high-performance file system that is designed for HPC workloads requiring rapid access to large datasets. The persistent file system maintains data even after reboots, which is necessary for a weather forecasting company that needs to process large amounts of data with high throughput and low latency.

561. Question #649 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?

- 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.

答案: C

解析: Option C, General Purpose SSD (gp3) EBS volume storage type, is the most cost-effective solution for the given requirements. GP3 EBS volumes provide a balance of performance and cost, allowing for the provision of 15,000 IOPS, which meets the company's needs without incurring the higher costs associated with io1 volumes or the potential over-provisioning of gp2 volumes.

解析: Option C, General Purpose SSD (gp3) EBS volume storage type, is the most cost-effective solution for the given requirements. GP3 EBS volumes provide a balance of performance and cost, allowing for the provision of 15,000 IOPS, which meets the company's needs without incurring the higher costs associated with io1 volumes or the potential over-provisioning of gp2 volumes.

562. Question #650A 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?

- 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

答案: A

解析: Option A, migrating to Amazon RDS for Microsoft SQL Server and using read replicas for reporting purposes, is the solution that will most likely reduce operational overhead. Amazon RDS is a managed service that handles time-consuming tasks such as hardware provisioning, database setup, patching, and backups. Read replicas can share the workload with the primary database, which helps in offloading read queries during reporting and analytical processing.

解析: Option A, migrating to Amazon RDS for Microsoft SQL Server and using read replicas for reporting purposes, is the solution that will most likely reduce operational overhead. Amazon RDS is a managed service that handles time-consuming tasks such as hardware provisioning, database

setup, patching, and backups. Read replicas can share the workload with the primary database, which helps in offloading read queries during reporting and analytical processing.

563. Question #651A 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**?

- 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.

答案: C

解析: Option C is the most cost-effective solution. It involves transitioning the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days when they are infrequently accessed, ensuring high availability and lower storage costs compared to S3 One Zone-IA. After 360 days, transitioning to S3 Glacier Instant Retrieval meets the requirement for instant availability upon request. Finally, after 5 years, moving the objects to S3 Glacier Deep Archive aligns with the need

for long-term archiving and retrieval within 12 hours by auditors, while still maintaining cost efficiency.

解析: Option C is the most cost-effective solution. It involves transitioning the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days when they are infrequently accessed, ensuring high availability and lower storage costs compared to S3 One Zone-IA. After 360 days, transitioning to S3 Glacier Instant Retrieval meets the requirement for instant availability upon request. Finally, after 5 years, moving the objects to S3 Glacier Deep Archive aligns with the need for long-term archiving and retrieval within 12 hours by auditors, while still maintaining cost efficiency.

564. Question #652A 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?

- 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.

答案: B

解析: Option B provides a balance between cost and data safety. By configuring a transient cluster with the primary node and core nodes on On-Demand Instances, the company ensures that the critical components of the EMR cluster are highly available and reliable. Using Spot Instances for task nodes allows for cost savings while still maintaining the ability to process large data workloads. Since the workload runs daily for a defined period, a transient cluster that scales down after use is

also a cost-effective choice.

解析: Option B provides a balance between cost and data safety. By configuring a transient cluster with the primary node and core nodes on On-Demand Instances, the company ensures that the critical components of the EMR cluster are highly available and reliable. Using Spot Instances for task nodes allows for cost savings while still maintaining the ability to process large data workloads. Since the workload runs daily for a defined period, a transient cluster that scales down after use is also a cost-effective choice.

565. Question #653A 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?

- 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.

答案: B

解析: Option B is the most suitable solution for automating the tagging of resources with the appropriate cost center ID. By creating a Lambda function that retrieves the cost center information from the RDS database and using an EventBridge rule to trigger this function in response to CloudTrail events, the company can ensure that resources are tagged correctly at the time of creation. This approach requires minimal manual intervention and provides a scalable solution for tagging resources across the organization.

解析: Option B is the most suitable solution for automating the tagging of resources with the appropriate cost center ID. By creating a Lambda function that retrieves the cost center information from the RDS database and using an EventBridge rule to trigger this function in response to CloudTrail events, the company can ensure that resources are tagged correctly at the time of creation. This approach requires minimal manual intervention and provides a scalable solution for tagging resources across the organization.

566. Question #654A 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?

- 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.

答案：D

解析：Option D provides a highly available and managed solution that meets the company's requirements. By using Amazon CloudFront to serve static content from Amazon S3, the company can ensure low latency and high availability for their static assets. For the PHP application, employing Amazon ECS with AWS Fargate removes the need to manage servers, and using an Application Load Balancer provides fault tolerance and traffic distribution. Additionally, configuring an ElastiCache for Redis cluster in multiple Availability Zones enhances the availability and performance of the session data.

解析：Option D provides a highly available and managed solution that meets the company's requirements. By using Amazon CloudFront to serve static content from Amazon S3, the company can ensure low latency and high availability for their static assets. For the PHP application, employing Amazon ECS with AWS Fargate removes the need to manage servers, and using an Application Load Balancer provides fault tolerance and traffic distribution. Additionally, configuring an ElastiCache for Redis cluster in multiple Availability Zones enhances the availability and performance of the session data.

567. Question #656A 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?

- 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.

答案: D

解析: Given that the images are requested infrequently—only once or twice a year—the most cost-effective solution is to store them in Amazon S3 Standard-Infrequent Access (S3 Standard-IA), as indicated in option D. This storage class is designed for data that is accessed less frequently, offering lower storage costs compared to S3 Standard while still providing the necessary durability and availability. Using S3 Standard-IA in conjunction with a static website hosted on Amazon S3 allows for direct delivery of images to users in a highly available manner.

解析: Given that the images are requested infrequently—only once or twice a year—the most cost-effective solution is to store them in Amazon S3 Standard-Infrequent Access (S3 Standard-IA), as indicated in option D. This storage class is designed for data that is accessed less frequently, offering lower storage costs compared to S3 Standard while still providing the necessary durability and availability. Using S3 Standard-IA in conjunction with a static website hosted on Amazon S3 allows for direct delivery of images to users in a highly available manner.

568. Question #657A 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?

- 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.

答案：B

解析：Option B is the most cost-effective solution for centralizing the management of security group rules across multiple AWS accounts and offices. By creating a customer managed prefix list containing the list of CIDRs and sharing it using AWS RAM, the company can ensure consistent security group configurations across the organization. This approach minimizes administrative overhead because any updates to the prefix list will automatically apply to all security groups that reference it, eliminating the need to update each security group individually.

解析：Option B is the most cost-effective solution for centralizing the management of security group rules across multiple AWS accounts and offices. By creating a customer managed prefix list containing the list of CIDRs and sharing it using AWS RAM, the company can ensure consistent security group configurations across the organization. This approach minimizes administrative overhead because any updates to the prefix list will automatically apply to all security groups that reference it, eliminating the need to update each security group individually.

569. Question #659A 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?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized**
- D. AWS Storage Gateway

答案: C

解析: Given the large amount of data (50 TB) that needs to be transferred within a tight timeframe (2 weeks) and the high utilization of the existing VPN connection, the most suitable solution is AWS Snowball Edge Storage Optimized (Option C). This service allows for fast data transfer through physical appliances that can be shipped to the customer's location for data ingestion, and then returned to AWS for uploading to the cloud. This approach bypasses the need to rely on the internet or the fully utilized VPN, and can significantly accelerate the data transfer process.

解析: Given the large amount of data (50 TB) that needs to be transferred within a tight timeframe (2 weeks) and the high utilization of the existing VPN connection, the most suitable solution is AWS Snowball Edge Storage Optimized (Option C). This service allows for fast data transfer through physical appliances that can be shipped to the customer's location for data ingestion, and then returned to AWS for uploading to the cloud. This approach bypasses the need to rely on the internet or the fully utilized VPN, and can significantly accelerate the data transfer process.

570. Question #660A 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?

- 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.

答案: D

解析: Since the peak hours occur at the same time each day and the performance issues are experienced at the start of these peak hours, a scheduled scaling policy (Option D) is the most appropriate solution. This allows the Auto Scaling group to launch new instances in anticipation of the increased load, ensuring that there is sufficient capacity to handle the peak traffic without performance degradation.

解析: Since the peak hours occur at the same time each day and the performance issues are experienced at the start of these peak hours, a scheduled scaling policy (Option D) is the most appropriate solution. This allows the Auto Scaling group to launch new instances in anticipation of the increased load, ensuring that there is sufficient capacity to handle the peak traffic without performance degradation.

571. Question #661A 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?**

- 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.

答案：B

解析：Amazon RDS Proxy (Option B) is designed to make applications more resilient to database failures and improve database efficiency by pooling and sharing connections. This fully managed service requires minimal operational overhead and integrates with existing RDS databases, making it an ideal solution for scaling the database connections without significant changes to the existing infrastructure or applications.

解析：Amazon RDS Proxy (Option B) is designed to make applications more resilient to database failures and improve database efficiency by pooling and sharing connections. This fully managed service requires minimal operational overhead and integrates with existing RDS databases, making it an ideal solution for scaling the database connections without significant changes to the existing infrastructure or applications.

572. Question #662A 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**?

- 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.

答案：D

解析：Option D provides a sustainable and automated approach to managing EBS snapshots, which can help optimize costs with minimal operational overhead. By deleting nonessential snapshots and using Amazon Data Lifecycle Manager (DLM) to automate the creation and deletion of snapshots, the company can enforce a snapshot policy that aligns with its cost optimization goals without requiring continuous manual intervention.

解析：Option D provides a sustainable and automated approach to managing EBS snapshots, which can help optimize costs with minimal operational overhead. By deleting nonessential snapshots and using Amazon Data Lifecycle Manager (DLM) to automate the creation and deletion of snapshots, the company can enforce a snapshot policy that aligns with its cost optimization goals without requiring continuous manual intervention.

573. Question #663A 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?

- 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.
- 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.

答案：D

解析：To ensure that only the Amazon ECS cluster can access the data in the RDS for MySQL database and the S3 bucket, while protecting sensitive information, I recommend using VPC endpoints and security groups. This solution aligns with the principle of least privilege and provides better network-level isolation. Here's a step-by-step guide to implement this solution:

1. Create a VPC Endpoint for Amazon RDS – Navigate to the VPC console (<https://console.aws.amazon.com/vpc/>) – Create an interface VPC endpoint for Amazon RDS – Associate the endpoint with the VPC where your ECS cluster is running – Ensure that the security group associated with the endpoint allows inbound traffic from the ECS cluster's security group
2. Configure RDS Security Group – Go to the RDS console (<https://console.aws.amazon.com/rds/>) – Modify the security group associated with your RDS for MySQL instance – Add an inbound rule that allows traffic only from the subnets where your ECS tasks will run – Specify the port for MySQL (typically 3306)
3. Create a VPC Endpoint for Amazon S3 – Return to the VPC console – Create a gateway VPC endpoint for Amazon S3 – Associate it with the VPC where your ECS cluster is running – Ensure that the route table for your ECS subnets includes a route to the S3 endpoint
4. Update S3 Bucket Policy – Go to the S3 console (<https://console.aws.amazon.com/s3/>) – Select your bucket and navigate to the Permissions tab – Edit the bucket policy to allow access only from your VPC endpoint – Include conditions to restrict access to the ECS task execution role
5. Configure ECS Task Execution Role – Navigate to the IAM console (<https://console.aws.amazon.com/iam/>) – Modify the ECS task execution role to include necessary permissions for S3 and RDS access – Ensure the role has the minimum required permissions following the principle of least privilege
6. Update ECS Task Definitions – Go to the ECS console (<https://console.aws.amazon.com/ecs/>) – Modify your task definitions to use the updated task execution role – Ensure that the task

definition includes the necessary environment variables or configuration to connect to RDS and S3 using the VPC endpoints. By implementing these steps, you'll create a secure environment where only your ECS cluster can access the sensitive data in the RDS for MySQL database and the S3 bucket. The use of VPC endpoints provides network-level isolation, while the security group and bucket policy configurations ensure fine-grained access control. Remember to test this configuration thoroughly in a non-production environment before implementing it in your production setup. Also, regularly review and audit your security settings to maintain a strong security posture.

Sources [1] [SEC08-BP02 Enforce encryption at rest – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2023-10-03/framework/sec_protect_data_rest_encrypt.html) [3] [Handling sensitive data – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/defining-bucket-names-data-lakes/handling-sensitive-data.html>) [6] [SEC08-BP02 Enforce encryption at rest – AWS Well-Architected Framework (2022-03-31)] (https://docs.aws.amazon.com/wellarchitected/2022-03-31/framework/sec_protect_data_rest_encrypt.html)

解析: To ensure that only the Amazon ECS cluster can access the data in the RDS for MySQL database and the S3 bucket, while protecting sensitive information, I recommend using VPC endpoints and security groups. This solution aligns with the principle of least privilege and provides better network-level isolation. Here's a step-by-step guide to implement this solution:

1. Create a VPC Endpoint for Amazon RDS – Navigate to the VPC console (<https://console.aws.amazon.com/vpc/>) – Create an interface VPC endpoint for Amazon RDS – Associate the endpoint with the VPC where your ECS cluster is running – Ensure that the security group associated with the endpoint allows inbound traffic from the ECS cluster's security group
2. Configure RDS Security Group – Go to the RDS console (<https://console.aws.amazon.com/rds/>) – Modify the security group associated with your RDS for MySQL instance – Add an inbound rule that allows traffic only from the subnets where your ECS tasks will run – Specify the port for MySQL (typically 3306)
3. Create a VPC Endpoint for Amazon S3 – Return to the VPC console – Create a

gateway VPC endpoint for Amazon S3 – Associate it with the VPC where your ECS cluster is running – Ensure that the route table for your ECS subnets includes a route to the S3 endpoint 4. Update S3 Bucket Policy – Go to the S3 console (<https://console.aws.amazon.com/s3/>) – Select your bucket and navigate to the Permissions tab – Edit the bucket policy to allow access only from your VPC endpoint – Include conditions to restrict access to the ECS task execution role 5. Configure ECS Task Execution Role – Navigate to the IAM console (<https://console.aws.amazon.com/iam/>) – Modify the ECS task execution role to include necessary permissions for S3 and RDS access – Ensure the role has the minimum required permissions following the principle of least privilege 6. Update ECS Task Definitions – Go to the ECS console (<https://console.aws.amazon.com/ecs/>) – Modify your task definitions to use the updated task execution role – Ensure that the task definition includes the necessary environment variables or configuration to connect to RDS and S3 using the VPC endpoints By implementing these steps, you'll create a secure environment where only your ECS cluster can access the sensitive data in the RDS for MySQL database and the S3 bucket. The use of VPC endpoints provides network-level isolation, while the security group and bucket policy configurations ensure fine-grained access control. Remember to test this configuration thoroughly in a non-production environment before implementing it in your production setup. Also, regularly review and audit your security settings to maintain a strong security posture.

Sources [1] [SEC08-BP02 Enforce encryption at rest – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2023-10-03/framework/sec_protect_data_rest_encrypt.html) [3] [Handling sensitive data – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/defining-bucket-names-data-lakes/handling-sensitive-data.html>) [6] [SEC08-BP02 Enforce encryption at rest – AWS Well-Architected Framework (2022-03-31)] (https://docs.aws.amazon.com/wellarchitected/2022-03-31/framework/sec_protect_data_rest_encrypt.html)

574. Question #664A 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?

- 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.

答案: D

解析: Option D is the most suitable solution for addressing the company's needs. By using burstable performance instances in unlimited mode, the application can handle sudden spikes in CPU utilization without being constrained by CPU credits. Configuring the environment to scale on predictive metrics allows Elastic Beanstalk to anticipate increased demand and scale the application proactively, which can help prevent latency issues during peak hours.

解析: Option D is the most suitable solution for addressing the company's needs. By using burstable performance instances in unlimited mode, the application can handle sudden spikes in CPU utilization without being constrained by CPU credits. Configuring the environment to scale on predictive metrics allows Elastic Beanstalk to anticipate increased demand and scale the application proactively, which can help prevent latency issues during peak hours.

575. Question #665A 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?

- 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.

答案：B

解析：Option B is the correct solution. AWS CloudFormation allows the company to automate the setup of its infrastructure as code, ensuring that configurations can be consistently applied and easily updated. AWS Config, on the other hand, is designed to track and audit all changes made to the resources within the AWS environment. This combination provides both the automation for infrastructure setup and the change tracking capabilities required by the security team.

解析：Option B is the correct solution. AWS CloudFormation allows the company to automate the setup of its infrastructure as code, ensuring that configurations can be consistently applied and easily updated. AWS Config, on the other hand, is designed to track and audit all changes made to the resources within the AWS environment. This combination provides both the automation for infrastructure setup and the change tracking capabilities required by the security team.

576. Question #667A 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?

- 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.

答案：C

解析：Option C is the correct solution. Interface endpoints for Amazon S3 allow for private connectivity between the VPC and Amazon S3 without data traversing the internet. Since the company has an AWS Direct Connect connection, interface endpoints can be used to provide secure access to S3 data from both the AWS Region and the on-premises location.

解析：Option C is the correct solution. Interface endpoints for Amazon S3 allow for private connectivity between the VPC and Amazon S3 without data traversing the internet. Since the company has an AWS Direct Connect connection, interface endpoints can be used to provide secure access to S3 data from both the AWS Region and the on-premises location.

577. Question #668A 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?

- 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.**

答案: D

解析: Option D, creating a tag policy in AWS Organizations, is the solution that meets the requirements. A tag policy can enforce the use of specific tags and their values across all accounts within an organization, ensuring that only resources with approved application names are created. This approach provides a centralized way to manage and enforce tagging standards without the need for per-account configurations.

解析: Option D, creating a tag policy in AWS Organizations, is the solution that meets the requirements. A tag policy can enforce the use of specific tags and their values across all accounts within an organization, ensuring that only resources with approved application names are created. This approach provides a centralized way to manage and enforce tagging standards without the need for per-account configurations.

578. Question #669A 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?

- 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.

答案: C

解析: Option C, integrating AWS Secrets Manager with Amazon RDS for PostgreSQL, is the solution that meets the requirements with the least operational overhead. AWS Secrets Manager automates the process of rotating the database credentials, including the master user password, without the need for manual intervention or custom scripting. This integration provides a secure and efficient way to manage database credentials.

解析: Option C, integrating AWS Secrets Manager with Amazon RDS for PostgreSQL, is the solution that meets the requirements with the least operational overhead. AWS Secrets Manager automates the process of rotating the database credentials, including the master user password, without the need for manual intervention or custom scripting. This integration provides a secure and efficient way to manage database credentials.

579. Question #670A 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?

- 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.

答案: B

解析: Option B, choosing provisioned mode and updating the read and write capacity units appropriately, is the most cost-effective solution for the given use case. Since the company has predictable workloads that occur once a week for a specific duration, it can provision the exact capacity needed for those 4 hours, avoiding the unnecessary costs associated with

on-demand mode or the commitment of reserved capacity for a longer term.

解析: Option B, choosing provisioned mode and updating the read and write capacity units appropriately, is the most cost-effective solution for the given use case. Since the company has predictable workloads that occur once a week for a specific duration, it can provision the exact capacity needed for those 4 hours, avoiding the unnecessary costs associated with on-demand mode or the commitment of reserved capacity for a longer term.

580. Question #671A 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?

- 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.

答案: B

解析: Option B, creating an AWS Cost Anomaly Detection monitor, is the solution that will meet the requirements. AWS Cost Anomaly Detection uses machine learning to identify and alert on unusual spending patterns, allowing the company to quickly respond to unexpected cost increases. This proactive monitoring and notification system is designed to prevent unusual spending by keeping stakeholders informed.

解析: Option B, creating an AWS Cost Anomaly Detection monitor, is the solution that will meet the requirements. AWS Cost Anomaly Detection uses machine learning to identify and alert on unusual spending patterns, allowing the company to quickly respond to unexpected cost increases. This proactive monitoring and notification system is designed to prevent unusual spending by keeping stakeholders informed.

581. Question #672A 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?

- 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.

答案：B

解析：Option B, configuring an AWS Glue crawler to crawl the data and using Amazon Athena to query the data, is the solution that meets the requirements with the least operational overhead. AWS Glue automates the data discovery and cataloging process, while Amazon Athena enables ad-hoc querying of data directly in Amazon S3 using standard SQL, without the need for additional setup or maintenance of a separate database or processing cluster.

解析：Option B, configuring an AWS Glue crawler to crawl the data and using Amazon Athena to query the data, is the solution that meets the requirements with the least operational overhead. AWS Glue automates the data discovery and cataloging process, while Amazon Athena enables ad-hoc querying of data directly in Amazon S3 using standard SQL, without the need for additional setup or maintenance of a separate database or processing cluster.

582. Question #673A 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?

- 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.

答案：B

解析：Option B is the correct solution. By creating an Amazon S3 File Gateway, the company can maintain access to the files via the SMB protocol while also integrating its storage with AWS. Setting up an S3 Lifecycle policy to transition data to S3 Glacier Deep Archive after 7 days meets the requirement for cost-effective storage and the ability to retrieve files within 24 hours when needed, as S3 Glacier Deep Archive offers retrieval options that can accommodate this retrieval time frame.

解析：Option B is the correct solution. By creating an Amazon S3 File Gateway, the company can maintain access to the files via the SMB protocol while also integrating its storage with AWS. Setting up an S3 Lifecycle policy to transition data to S3 Glacier Deep Archive after 7 days meets the requirement for cost-effective storage and the ability to retrieve files within 24 hours when needed, as S3 Glacier Deep Archive offers retrieval options that can accommodate this retrieval time frame.

583. Question #675A 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?

- 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.

答案：D

解析：Option D, locking the EBS snapshots, is the solution that requires the least administrative effort. By using the snapshot lock feature, the company can prevent accidental deletions without affecting the existing permissions and administrative rights of the storage administrator. This approach provides a straightforward and effective way to protect the snapshots.

解析：Option D, locking the EBS snapshots, is the solution that requires the least administrative effort. By using the snapshot lock feature, the company can prevent accidental deletions without affecting the existing permissions and administrative rights of the storage administrator. This approach provides a straightforward and effective way to protect the snapshots.

584. Question #676A 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?

- 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.

答案：B

解析：Option B is the correct solution. By configuring VPC Flow Logs to send the log data to a log group in Amazon CloudWatch Logs, the company can capture information about the network traffic. Then, using Amazon Kinesis Data Firehose, the company can stream the logs to Amazon OpenSearch Service for near real-time analysis. Kinesis Data Firehose is a fully managed service that is designed for this purpose and requires less administrative overhead compared to setting up and managing a Kinesis Data Streams solution.

解析：Option B is the correct solution. By configuring VPC Flow Logs to send the log data to a log group in Amazon CloudWatch Logs, the company can capture information about the network traffic. Then, using Amazon Kinesis Data Firehose, the company can stream the logs to Amazon OpenSearch Service for near real-time analysis. Kinesis Data Firehose is a fully managed service that is designed for this purpose and requires less administrative overhead compared to setting up and managing a Kinesis Data Streams solution.

585. Question #677A 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?**

- 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.

答案：B

解析：Option B provides a cost-effective solution by combining the use of On-Demand Instances and Spot Instances across two managed node groups. The On-Demand Instances ensure that the development cluster has the necessary, reliable compute capacity for critical tasks, while the Spot Instances can be used for less critical, cost-saving purposes. This approach balances the need for reliability with the potential cost savings from Spot Instances.

解析：Option B provides a cost-effective solution by combining the use of On-Demand Instances and Spot Instances across two managed node groups. The On-Demand Instances ensure that the development cluster has the necessary, reliable compute capacity for critical tasks, while the Spot Instances can be used for less critical, cost-saving purposes. This approach balances the need for reliability with the potential cost savings from Spot Instances.

586. Question #678A 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?

- 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.

答案：B

解析：Option B, creating a customer managed key with AWS KMS and using it for SSE-KMS, provides the company with full control over the encryption keys. This includes the ability to create, rotate, and disable keys as needed. By managing the keys within AWS KMS, the company can also take advantage of the integrated key management capabilities, such as key policy management and access control, without the need for manual intervention in the encryption process.

解析：Option B, creating a customer managed key with AWS KMS and using it for SSE-KMS, provides the company with full control over the encryption keys. This includes the ability to create, rotate, and disable keys as needed. By managing the keys within AWS KMS, the company can also take advantage of the integrated key management capabilities, such as key policy management and access control, without the need for manual intervention in the encryption process.

587. Question #680A 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?

- 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.

答案：A

解析：Option A, using AWS DataSync, is the solution that meets the requirements with the least operational overhead. DataSync is designed to automatically transfer files based on set tasks and can be configured to only transfer data that has changed, thereby minimizing the amount of data being moved and reducing operational overhead. By creating tasks for both the destination S3 bucket and the EFS file system, the architect can ensure continuous and efficient synchronization.

解析：Option A, using AWS DataSync, is the solution that meets the requirements with the least operational overhead. DataSync is designed to automatically transfer files based on set tasks and can be configured to only transfer data that has changed, thereby minimizing the amount of data being moved and reducing operational overhead. By creating tasks for both the destination S3 bucket and the EFS file system, the architect can ensure continuous and efficient synchronization.

588. Question #681A 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?**

- 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.

答案：A

解析：Based on the company's requirements to encrypt data at rest using AWS KMS and control the rotation of encryption keys, the best solution with the least operational overhead is: A. Create a customer managed key. Use the key to encrypt the EBS volumes. Here's why this is the most suitable option:

1. Encryption at rest: Customer managed keys in AWS KMS can be used to encrypt EBS volumes, ensuring data is encrypted at rest.
2. Control over key rotation: With customer managed keys, the company has full control over key rotation. They can set up automatic key rotation or manually rotate keys according to their security policies.
3. Least operational overhead: While creating a customer managed key requires some initial setup, it provides the best balance between control and ease of management. AWS manages the underlying infrastructure and security of the key material.
4. Flexibility: Customer managed keys offer more flexibility in terms of key policies, auditing, and integration with other AWS services.
5. Compliance: Using customer managed keys can help meet various compliance requirements that mandate control over encryption keys.

To implement this solution:

1. Create a customer managed key in AWS KMS for the specific region where the EBS volumes are located.
2. Configure the key policy to allow appropriate access for necessary IAM roles and users.
3. When creating new EBS volumes or modifying existing ones, specify this customer managed key for encryption.
4. Optionally, set up automatic key rotation (recommended) or implement a process for manual rotation.

Sources [1] [Amazon EBS volume encryption – AWS Key Management Service] (<https://docs.aws.amazon.com/kms/latest/cryptographic-details/ebs-volume-encryption.html>) [3] [How Amazon EBS encryption works – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/how-ebs-encryption-works.html>) [6] [Data protection in Amazon EBS – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/data-protection.html>)

解析：Based on the company's requirements to encrypt data at rest using AWS KMS and control the rotation of encryption keys, the best solution

with the least operational overhead is:

- A. Create a customer managed key. Use the key to encrypt the EBS volumes. Here's why this is the most suitable option:
 1. Encryption at rest: Customer managed keys in AWS KMS can be used to encrypt EBS volumes, ensuring data is encrypted at rest.
 2. Control over key rotation: With customer managed keys, the company has full control over key rotation. They can set up automatic key rotation or manually rotate keys according to their security policies.
 3. Least operational overhead: While creating a customer managed key requires some initial setup, it provides the best balance between control and ease of management. AWS manages the underlying infrastructure and security of the key material.
 4. Flexibility: Customer managed keys offer more flexibility in terms of key policies, auditing, and integration with other AWS services.
 5. Compliance: Using customer managed keys can help meet various compliance requirements that mandate control over encryption keys.

To implement this solution:

1. Create a customer managed key in AWS KMS for the specific region where the EBS volumes are located.
2. Configure the key policy to allow appropriate access for necessary IAM roles and users.
3. When creating new EBS volumes or modifying existing ones, specify this customer managed key for encryption.
4. Optionally, set up automatic key rotation (recommended) or implement a process for manual rotation.

Sources [1] [Amazon EBS volume encryption – AWS Key Management Service] (<https://docs.aws.amazon.com/kms/latest/cryptographic-details/ebs-volume-encryption.html>) [3] [How Amazon EBS encryption works – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/how-ebs-encryption-works.html>) [6] [Data protection in Amazon EBS – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/data-protection.html>)

589. Question #682A 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?**

- 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.

答案：A

解析：Option A provides a straightforward and automated approach to enforce data encryption at rest on Amazon EC2 instances. By using an IAM policy to restrict the creation of only encrypted EBS volumes, the company can prevent the introduction of unencrypted resources. AWS Config can then be used to monitor and assess the compliance of existing resources, while AWS Systems Manager Automation can remediate any noncompliant resources automatically, leading to minimal administrative overhead.

解析：Option A provides a straightforward and automated approach to enforce data encryption at rest on Amazon EC2 instances. By using an IAM policy to restrict the creation of only encrypted EBS volumes, the company can prevent the introduction of unencrypted resources. AWS Config can then be used to monitor and assess the compliance of existing resources, while AWS Systems Manager Automation can remediate any noncompliant resources automatically, leading to minimal administrative overhead.

590. Question #684A 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?

- 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.

答案: D

解析: To achieve the required low latency and comply with regulations that prevent the use of the eu-central-1 Region for some applications, the company should deploy the applications in AWS Wavelength Zones (Option D). Wavelength Zones are AWS infrastructure deployments within telecommunications providers' facilities, bringing AWS services closer to the end-users and providing single-digit millisecond latency. By extending the company's VPC to a chosen Wavelength Zone, the company can maintain compliance and achieve the desired performance.

解析: To achieve the required low latency and comply with regulations that prevent the use of the eu-central-1 Region for some applications, the company should deploy the applications in AWS Wavelength Zones (Option D). Wavelength Zones are AWS infrastructure deployments within telecommunications providers' facilities, bringing AWS services closer to the end-users and providing single-digit millisecond latency. By extending the company's VPC to a chosen Wavelength Zone, the company can maintain compliance and achieve the desired performance.

591. #Question #685A 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?

- 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.

答案：B

解析：To maintain predictable database performance and prevent overloading the database with too many connections, a solutions architect should use an RDS proxy endpoint. This is because an RDS proxy can manage and limit the number of connections to the database, thus preventing the Lambda functions from overwhelming the database. Additionally, **deploying the Lambda functions inside a VPC ensures that the connections are secure and within the AWS network environment, which is not possible if the Lambda functions are deployed outside a VPC.**

解析：To maintain predictable database performance and prevent overloading the database with too many connections, a solutions architect should use an RDS proxy endpoint. This is because an RDS proxy can manage and limit the number of connections to the database, thus preventing the Lambda functions from overwhelming the database. Additionally, deploying the Lambda functions inside a VPC ensures that the connections are secure and within the AWS network environment, which is not possible if the Lambda functions are deployed outside a VPC.

592. #Question #686A 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?**

- 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.

答案：C

解析：The solution that would meet the requirements of simplifying the administration of new connections and providing scalability with the least administrative overhead is to create a transit gateway (Option C). A transit gateway acts as a hub and spoke model, allowing multiple VPCs and on-premises locations to connect in a single point, which simplifies network management and reduces the overhead of setting up individual peering or VPN connections for each.

解析：The solution that would meet the requirements of simplifying the administration of new connections and providing scalability with the least administrative overhead is to create a transit gateway (Option C). A transit gateway acts as a hub and spoke model, allowing multiple VPCs and on-premises locations to connect in a single point, which simplifies network management and reduces the overhead of setting up individual peering or VPN connections for each.

593. #Question #688A 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?**

- 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.

答案: C

解析: To manage permissions across multiple AWS accounts with the least operational overhead, the company should use IAM Identity Center's permission sets (Option C). By creating permission sets for developers and administrators, the company can easily assign the correct set of permissions to new users or groups without having to manage individual policies for each user. This approach also simplifies the process of adding new users to the appropriate group, ensuring they have the necessary permissions across all accounts.

解析: To manage permissions across multiple AWS accounts with the least operational overhead, the company should use IAM Identity Center's permission sets (Option C). By creating permission sets for developers and administrators, the company can easily assign the correct set of permissions to new users or groups without having to manage individual policies for each user. This approach also simplifies the process of

adding new users to the appropriate group, ensuring they have the necessary permissions across all accounts.

594. #Question #689A 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?
- 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.

答案: D

解析: 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. 这个选项建议编写API调用来描述EBS卷并确认它们是否已加密。然后，使用EventBridge来调度Lambda函数以运行这些API调用。优点：可以实现自动化检查，并且Lambda函数可以按需运行，降低成本。

缺点：需要编写和维护Lambda函数，以及设置EventBridge规则，这可能需要一定的配置工作。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. 这个选项与A类似，但使用Fargate任务来运行API调用。

优点：Fargate可以提供计算资源而无需管理服务器或集群。

缺点：相比于Lambda，Fargate可能更加昂贵，并且需要更多的配置和管理工作。

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. 这个选项建议通过IAM策略强制对EBS卷进行标记，并使用Cost

Explorer来识别未正确标记的资源。

优点：通过标记可以更容易地管理和追踪资源。 缺点：这种方法并不能直接解决加密检查的问题，而且手动加密可能会增加操作成本。 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. 这个选项建议使用AWS Config规则来自动检查EBS卷是否已加密，并在未加密时标记该卷。 优点：AWS Config可以自动、持续地监控AWS资源，并可以在不满足特定条件时触发警报或自动修复。这种方法既简化了加密检查，又降低了运营成本。

缺点：可能需要一些初始配置来设置AWS Config规则。 参考答案：

考虑到公司想要标准化其Amazon EBS卷加密策略，并最小化运营卷加密检查的成本和配置工作，选项D是最合适的解决方案。通过使用AWS Config规则，公司可以自动化地检查EBS卷的加密状态，并在未加密时进行标记，从而满足其标准化和成本最小化的要求。 因此，答案是 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.

解析：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. 这个选项建议编写API调用来描述EBS卷并确认它们是否已加密。然后，使用EventBridge来调度Lambda函数以运行这些API调用。 优点：可以实现自动化检查，并且Lambda函数可以按需运行，降低成本。 缺点：需要编写和维护Lambda函数，以及设置EventBridge规则，这可能需要一定的配置工作。 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. 这个选项与A类似，但使用Fargate任务来运行API调用。

优点：Fargate可以提供计算资源而无需管理服务器或集群。

缺点：相比于Lambda，Fargate可能更加昂贵，并且需要更多的配置和管理工作。

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. 这个选项建议通过IAM策略强制对EBS卷进行标记，并使用Cost Explorer来识别未正确标记的资源。

优点：通过标记可以更容易地管理和追踪资源。 缺点：这种方法并不能直接解决加密检查的问题，而且手动加密可能会增加操作成本。 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. 这个选项建议使用AWS Config规则来自动检查EBS卷是否已加密，并在未加密时标记该卷。优点：AWS Config可以自动、持续地监控AWS资源，并可以在不满足特定条件时触发警报或自动修复。这种方法既简化了加密检查，又降低了运营成本。

缺点：可能需要一些初始配置来设置AWS Config规则。参考答案：

考虑到公司想要标准化其Amazon EBS卷加密策略，并最小化运营卷加密检查的成本和配置工作，选项D是最合适的解决方案。通过使用AWS Config规则，公司可以自动化地检查EBS卷的加密状态，并在未加密时进行标记，从而满足其标准化和成本最小化的要求。因此，答案是 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.

595. #Question #692A 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?

- 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.

答案：A

解析：To provide the most high-performing experience, the architect should use Amazon Route 53's latency-based routing policy (Option A). This policy routes users to the application endpoint that provides the lowest latency, which typically correlates with the best performance. Geolocation routing (Option B) is more suitable for location-specific content delivery rather than performance optimization. Failover and geoproximity policies (Options C and D) are more focused on availability and geographic proximity rather than performance.

解析：To provide the most high-performing experience, the architect should use Amazon Route 53's latency-based routing policy (Option A). This policy routes users to the application endpoint that provides the lowest latency, which typically correlates with the best performance.

Geolocation routing (Option B) is more suitable for location-specific content delivery rather than performance optimization. Failover and geoproximity policies (Options C and D) are more focused on availability and geographic proximity rather than performance.

596. #Question #693A 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**?

- 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).

答案：D

解析：To achieve high availability and eventual consistency with the least operational overhead, the solution is to modify the Auto Scaling group to span multiple Availability Zones (Option D) and migrate the embedded NoSQL database to Amazon DynamoDB, which is a managed service that provides high availability and eventual consistency by default. This migration can be facilitated with AWS DMS, which would reduce the overhead of managing replication and scaling compared to maintaining the embedded database.

解析：To achieve high availability and eventual consistency with the least operational overhead, the solution is to modify the Auto Scaling

group to span multiple Availability Zones (Option D) and migrate the embedded NoSQL database to Amazon DynamoDB, which is a managed service that provides high availability and eventual consistency by default. This migration can be facilitated with AWS DMS, which would reduce the overhead of managing replication and scaling compared to maintaining the embedded database.

597. #Question #694A 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?

- 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.

答案：B

解析：To ensure that shopping cart data is preserved at all times with high availability and low latency, the architect should configure Amazon ElastiCache for Redis (Option B). This service can be used to cache both catalog data and user session data, including shopping cart information, which allows for quick access and data persistence even if the user disconnects. This approach also helps to reduce the load on the database, thereby improving application performance.

解析：To ensure that shopping cart data is preserved at all times with high availability and low latency, the architect should configure Amazon ElastiCache for Redis (Option B). This service can be used to cache both

catalog data and user session data, including shopping cart information, which allows for quick access and data persistence even if the user disconnects. This approach also helps to reduce the load on the database, thereby improving application performance.

598. #Question #695A 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?

- 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.

答案：B

解析：To make the microservices-based application on Amazon EKS observable and to identify potential performance issues, the architect should configure Amazon CloudWatch Container Insights (Option B) to collect metrics from the EKS clusters. Additionally, AWS X-Ray should be configured to trace the requests between the microservices, providing insights into the interactions and performance of the application components.

解析：To make the microservices-based application on Amazon EKS observable and to identify potential performance issues, the architect should configure Amazon CloudWatch Container Insights (Option B) to collect metrics from the EKS clusters. Additionally, AWS X-Ray should be configured to trace the requests between the microservices, providing insights into the interactions and performance of the application

components.

599. #Question #696A 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?

- 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.

答案: C

解析: To meet the requirements for secure and customer-specific access to data stored in an Amazon S3 bucket, the solution is to provision a separate AWS KMS key for each customer (Option C). The data should be encrypted server-side using the KMS keys, ensuring that it is encrypted at rest. Then, in the policy associated with each KMS key, permissions should be restricted such that only an IAM role provided by the customer can decrypt the data. This approach ensures that only authorized customers can access their data, and company employees are prevented from

accessing it.

解析: To meet the requirements for secure and customer-specific access to data stored in an Amazon S3 bucket, the solution is to provision a separate AWS KMS key for each customer (Option C). The data should be encrypted server-side using the KMS keys, ensuring that it is encrypted at rest. Then, in the policy associated with each KMS key, permissions should be restricted such that only an IAM role provided by the customer can decrypt the data. This approach ensures that only authorized customers can access their data, and company employees are prevented from accessing it.

600. #Question #697A 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?

- 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.

答案: B

解析: To allow external internet traffic to connect to a web server hosted on an EC2 instance within a private subnet, the architect should provision an internet-facing Application Load Balancer (ALB) in a public subnet (Option B). The ALB can route traffic to the EC2 instance in the private subnet and act as the entry point for the web traffic.

Additionally#Question #697 (Continued) Additionally, the ALB can be configured with a security group that allows incoming traffic on ports 80 and 443, and the DNS record for the website should be set to resolve to the ALB's public-facing DNS name. This ensures that the web server is accessible over the internet while maintaining the security mandate of keeping the EC2 instance within a private subnet.

解析: To allow external internet traffic to connect to a web server hosted on an EC2 instance within a private subnet, the architect should provision an internet-facing Application Load Balancer (ALB) in a public subnet (Option B). The ALB can route traffic to the EC2 instance in the private subnet and act as the entry point for the web traffic.

Additionally#Question #697 (Continued) Additionally, the ALB can be configured with a security group that allows incoming traffic on ports 80 and 443, and the DNS record for the website should be set to resolve to the ALB's public-facing DNS name. This ensures that the web server is accessible over the internet while maintaining the security mandate of keeping the EC2 instance within a private subnet.

601. #Question #698A 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**?

- 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.

答案：B

解析：To meet the requirements for a highly available, fault-tolerant storage solution that can be shared between multiple containers with minimal operational overhead, the architect should choose Amazon EFS (Option B). EFS is designed to be scalable and highly available, and it can be mounted on multiple EC2 instances simultaneously, making it ideal for shared storage in a containerized environment like EKS. Using a single EFS file system for all containers simplifies management and ensures that data is consistent across all instances of the application.

解析：To meet the requirements for a highly available, fault-tolerant storage solution that can be shared between multiple containers with minimal operational overhead, the architect should choose Amazon EFS (Option B). EFS is designed to be scalable and highly available, and it can be mounted on multiple EC2 instances simultaneously, making it ideal for shared storage in a containerized environment like EKS. Using a single EFS file system for all containers simplifies management and ensures that data is consistent across all instances of the application.

602. #Question #699A 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?

- 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.

答案：B

解析：To move the application to a fully managed service without managing servers or storage infrastructure, the company should use Amazon ECS with AWS Fargate (Option B). Fargate is a serverless offering for ECS that removes the need to manage EC2 instances. By creating an Amazon EFS volume and using it as a persistent storage volume, the company can maintain the persistent data storage required by the application. This solution provides a fully managed environment for running containerized applications while still allowing for persistent storage.

解析：To move the application to a fully managed service without managing servers or storage infrastructure, the company should use Amazon ECS with AWS Fargate (Option B). Fargate is a serverless offering for ECS that removes the need to manage EC2 instances. By creating an Amazon EFS volume and using it as a persistent storage volume, the company can maintain the persistent data storage required by the application. This solution provides a fully managed environment for running containerized applications while still allowing for persistent storage.

603. #Question #701A 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?

- 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.

答案: C

解析: To address the issue of DDoS attacks with minimal configuration changes and to gain access to an audit trail for the attack sources, the city should subscribe to AWS Shield Advanced (Option C). **AWS Shield Advanced provides automatic DDoS attack detection and mitigation, and it includes support from the AWS DDoS Response Team.** This solution is specifically designed to protect web applications from DDoS attacks and requires less adjustment to the existing infrastructure compared to setting up AWS WAF rules or using Amazon Inspector.

解析: To address the issue of DDoS attacks with minimal configuration changes and to gain access to an audit trail for the attack sources, the city should subscribe to AWS Shield Advanced (Option C). **AWS Shield Advanced provides automatic DDoS attack detection and mitigation, and it includes support from the AWS DDoS Response Team.** This solution is specifically designed to protect web applications from DDoS attacks and requires less adjustment to the existing infrastructure compared to setting up AWS WAF rules or using Amazon Inspector.

604. #Question #702A 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?

- 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.

答案: D

解析: To achieve the required sub-millisecond latency and high-throughput access for the HPC cluster, the architect should directly import the data into an Amazon FSx for Lustre file system (Option D). FSx for Lustre is a high-performance file system designed for HPC environments and is optimized for workloads that demand fast access to large data sets. By bypassing intermediate storage layers and integrating FSx for Lustre directly with the HPC cluster, the architect can ensure the performance needs are met without the additional latency that might be introduced by other storage solutions or data transfer steps.

解析: To achieve the required sub-millisecond latency and high-throughput access for the HPC cluster, the architect should directly import the data

into an Amazon FSx for Lustre file system (Option D). FSx for Lustre is a high-performance file system designed for HPC environments and is optimized for workloads that demand fast access to large data sets. By bypassing intermediate storage layers and integrating FSx for Lustre directly with the HPC cluster, the architect can ensure the performance needs are met without the additional latency that might be introduced by other storage solutions or data transfer steps.

605. #Question #703A 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?
- 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.

答案：B

解析：The most cost-effective solution for periodically backing up small amounts of data from on-premises NFS servers to Amazon S3 is to set up an AWS DataSync agent (Option B). DataSync is designed for data transfer tasks and can efficiently synchronize files between on-premises storage and S3, even for recurring jobs. AWS Glue (Option A) is more suited for data extraction, transformation, and loading tasks rather than direct file synchronization. Using AWS Transfer for SFTP (Option C) would be an overkill for the scenario described, as it is designed for larger-scale file transfers and would incur higher costs. Establishing an AWS Direct Connect connection (Option D) is typically used for larger, more frequent data transfers and would represent a higher initial setup cost and operational overhead for the task of periodically backing up small amounts of data.

解析: The most cost-effective solution for periodically backing up small amounts of data from on-premises NFS servers to Amazon S3 is to set up an AWS DataSync agent (Option B). DataSync is designed for data transfer tasks and can efficiently synchronize files between on-premises storage and S3, even for recurring jobs. AWS Glue (Option A) is more suited for data extraction, transformation, and loading tasks rather than direct file synchronization. Using AWS Transfer for SFTP (Option C) would be an overkill for the scenario described, as it is designed for larger-scale file transfers and would incur higher costs. Establishing an AWS Direct Connect connection (Option D) is typically used for larger, more frequent data transfers and would represent a higher initial setup cost and operational overhead for the task of periodically backing up small amounts of data.

606. #Question #704 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?

- 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.

答案: C

解析: For handling millions of UDP traffic requests with ultra-low latency, a Network Load Balancer (Option C) is the most suitable and cost-effective solution. NLB is designed to handle high volumes of traffic and provides low latency, which is crucial for real-time applications like online gaming. Application Load Balancers (Option A) are optimized for HTTP/HTTPS traffic and are not as efficient for raw

data protocols like UDP. Gateway Load Balancers (Option B) operate at the network edge and are not designed for the low-level processing required for UDP traffic. Launching game servers in multiple Regions (Option D) would increase latency due to the increased complexity and geographic distribution, and it would not be as cost-effective as using a Network Load Balancer.

解析: For handling millions of UDP traffic requests with ultra-low latency, a Network Load Balancer (Option C) is the most suitable and cost-effective solution. NLB is designed to handle high volumes of traffic and provides low latency, which is crucial for real-time applications like online gaming. Application Load Balancers (Option A) are optimized for HTTP/HTTPS traffic and are not as efficient for raw data protocols like UDP. Gateway Load Balancers (Option B) operate at the network edge and are not designed for the low-level processing required for UDP traffic. Launching game servers in multiple Regions (Option D) would increase latency due to the increased complexity and geographic distribution, and it would not be as cost-effective as using a Network Load Balancer.

607. #Question #706A 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?

- 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.

答案：B

解析：The solution that will improve application performance with the least operational overhead is to create a read replica of the database (Option B). By offloading the read operations to the read replica, the primary database instance can maintain better performance for the critical application. This approach requires minimal changes to the existing infrastructure and leverages Amazon RDS's built-in replication capabilities. Adding functionality to the script (Option A) could be more complex and less reliable. Manually exporting data (Option C) is not efficient or scalable. Using Amazon ElastiCache (Option D) could help with caching frequent queries, but it would not directly address the issue of the script's impact on database performance.

解析：The solution that will improve application performance with the least operational overhead is to create a read replica of the database (Option B). By offloading the read operations to the read replica, the primary database instance can maintain better performance for the critical application. This approach requires minimal changes to the existing infrastructure and leverages Amazon RDS's built-in replication capabilities. Adding functionality to the script (Option A) could be more complex and less reliable. Manually exporting data (Option C) is not efficient or scalable. Using Amazon ElastiCache (Option D) could help with caching frequent queries, but it would not directly address the issue of the script's impact on database performance.

608. #Question #707A 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?**

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.

答案: B

解析: The most operationally efficient solution to improve visibility into the ALB's traffic is to enable access logging to Amazon S3 (Option B) and then create a table in Amazon Athena to query the logs. This method automates the process of analyzing traffic patterns and leverages Amazon Athena's ability to perform analytics directly on data stored in S3. Creating a table in Athena for CloudTrail logs (Option A) would not be as relevant since CloudTrail logs are more focused on API calls rather than ALB access patterns. Manually searching through log files in a text editor (Option C) is not a scalable or efficient approach. Using Amazon EMR (Option D) to query the ALB directly is unnecessary and would incur higher costs and complexity for the task at hand.

解析: The most operationally efficient solution to improve visibility into the ALB's traffic is to enable access logging to Amazon S3 (Option B) and then create a table in Amazon Athena to query the logs. This method automates the process of analyzing traffic patterns and leverages Amazon Athena's ability to perform analytics directly on data stored in S3. Creating a table in Athena for CloudTrail logs (Option A) would not be as relevant since CloudTrail logs are more focused on API calls rather than ALB access patterns. Manually searching through log files in a text editor (Option C) is not a scalable or efficient approach. Using Amazon EMR (Option D) to query the ALB directly is unnecessary and would incur higher costs and complexity for the task at hand.

609. #Question #708A 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?

- 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.

答案: C

解析: To allow Amazon EC2 instances in private subnets to connect to the public internet, the company should create public NAT gateways in public subnets (Option C). This setup enables the private instances to use the NAT gateway to access the internet while remaining isolated from direct public access. Creating public NAT gateways in private subnets (Option A) or private NAT gateways in either private (Option B) or public subnets (Option D) would not effectively provide internet access to the instances in private subnets, as private NAT gateways are not intended to provide internet access.

解析: To allow Amazon EC2 instances in private subnets to connect to the public internet, the company should create public NAT gateways in public subnets (Option C). This setup enables the private instances to use the NAT gateway to access the internet while remaining isolated from direct public access. Creating public NAT gateways in private subnets (Option A) or private NAT gateways in either private (Option B) or public subnets (Option D) would not effectively provide internet access to the instances in private subnets, as private NAT gateways are not intended to provide internet access.

610. #Question #710A 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?

- 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.

答案：A

解析：To establish a private and secure connection between Amazon EC2 instances and Amazon S3, the company should set up S3 bucket policies to allow access from a VPC endpoint (Option A). A VPC endpoint for S3 enables private connectivity between the VPC and S3 without requiring access over the public internet, thereby enhancing security. Setting up IAM policies (Option B) would only control access permissions but not establish a private connection. A NAT gateway (Option C) is used for accessing the internet and does not provide a private connection to AWS services. Using access keys (Option D) would provide authentication to S3 but not a private connection.

解析：To establish a private and secure connection between Amazon EC2 instances and Amazon S3, the company should set up S3 bucket policies to allow access from a VPC endpoint (Option A). A VPC endpoint for S3 enables private connectivity between the VPC and S3 without requiring access over the public internet, thereby enhancing security. Setting up IAM policies (Option B) would only control access permissions but not establish a private connection. A NAT gateway (Option C) is used for accessing the internet and does not provide a private connection to AWS services. Using access keys (Option D) would provide authentication to S3 but not a private connection.

611. #Question #711An 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**?

- 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.

答案: C

解析: To address the heavy read load and improve the scalability and high availability of the application with the least downtime, the architect should add additional reader instances to the Aurora cluster (Option C). This approach allows the database to handle more read traffic by distributing it across multiple reader instances. Additionally, creating an Amazon RDS Proxy for the Aurora cluster helps manage connections and provides a single point of access to the reader instances, further enhancing scalability and performance. Using Amazon EventBridge and AWS Lambda (Option A) would provide monitoring but not directly address the read load issue. Activating the ZDR feature (Option B) is more relevant to managing instance failures rather than read load. **Using ElastiCache (Option D) would introduce complexity and require additional replication management.**

解析: To address the heavy read load and improve the scalability and high availability of the application with the least downtime, the architect should add additional reader instances to the Aurora cluster (Option C). This approach allows the database to handle more read traffic by distributing it across multiple reader instances. Additionally, creating an Amazon RDS Proxy for the Aurora cluster helps manage connections and provides a single point of access to the reader instances, further enhancing scalability and performance. Using Amazon EventBridge and AWS

Lambda (Option A) would provide monitoring but not directly address the read load issue. Activating the ZDR feature (Option B) is more relevant to managing instance failures rather than read load. Using ElastiCache (Option D) would introduce complexity and require additional replication management.

612. #Question #712A 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?

- 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

答案：A

解析：To securely communicate with on-premises services from a VPC using private DNS records, the company should create a Route 53 Resolver outbound endpoint (Option A). This endpoint allows DNS queries to be made from the VPC to the on-premises network or another VPC over the VPN connection. A resolver rule is then used to define how the DNS queries should be routed. Associating the resolver rule with the VPC ensures that the private DNS records are used for communication, which is more secure than using a public hosted zone (Option D) or a private hosted zone without an outbound endpoint (Option C). Creating an inbound endpoint (Option B) would facilitate the opposite direction of communication, from on-premises to the VPC, which is not required by the scenario.

解析：To securely communicate with on-premises services from a VPC using private DNS records, the company should create a Route 53 Resolver

outbound endpoint (Option A). This endpoint allows DNS queries to be made from the VPC to the on-premises network or another VPC over the VPN connection. A resolver rule is then used to define how the DNS queries should be routed. Associating the resolver rule with the VPC ensures that the private DNS records are used for communication, which is more secure than using a public hosted zone (Option D) or a private hosted zone without an outbound endpoint (Option C). Creating an inbound endpoint (Option B) would facilitate the opposite direction of communication, from on-premises to the VPC, which is not required by the scenario.

613. #Question #713A 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**?

- 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.

答案：B

解析：The most cost-effective solution for storing photos with varying access patterns is to use Amazon S3 Intelligent-Tiering (Option B). This storage class automatically moves objects between two access tiers based on access frequency, which aligns with the description of the photo

viewing patterns. Storing the photo metadata and S3 location in DynamoDB allows for efficient querying and retrieval of photo information. Using DynamoDB Accelerator (Option A) would be unnecessary and more costly for this use case. Storing photos in S3 Standard and then moving them to Standard-IA or Glacier (Options C and D) would not be as cost-effective, as the per-request costs for data retrieval from these storage classes are higher compared to Intelligent-Tiering.

解析：The most cost-effective solution for storing photos with varying access patterns is to use Amazon S3 Intelligent-Tiering (Option B). This storage class automatically moves objects between two access tiers based on access frequency, which aligns with the description of the photo viewing patterns. Storing the photo metadata and S3 location in DynamoDB allows for efficient querying and retrieval of photo information. Using DynamoDB Accelerator (Option A) would be unnecessary and more costly for this use case. Storing photos in S3 Standard and then moving them to Standard-IA or Glacier (Options C and D) would not be as cost-effective, as the per-request costs for data retrieval from these storage classes are higher compared to Intelligent-Tiering.

614. #Question #714A 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?

- 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.

答案: D

解析: To prevent new requests from being forwarded to overloaded EC2 instances, the company should use the least outstanding requests algorithm (Option D) with the RequestCount and TargetResponseTime CloudWatch metrics. This algorithm routes requests to the targets with the lowest number of in-progress requests, which helps to distribute the load more evenly across instances and prevents overloading those that are already processing many requests. The round robin algorithm (Options A and C) does not consider the current load on the instances and would not be as effective in distributing the traffic to prevent overloading.

解析: To prevent new requests from being forwarded to overloaded EC2 instances, the company should use the least outstanding requests algorithm (Option D) with the RequestCount and TargetResponseTime CloudWatch metrics. This algorithm routes requests to the targets with the lowest number of in-progress requests, which helps to distribute the load more evenly across instances and prevents overloading those that are already processing many requests. The round robin algorithm (Options A and C) does not consider the current load on the instances and would not be as effective in distributing the traffic to prevent overloading.

615. #Question #715A 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?

- 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.

答案: A

解析: The most operationally efficient solution to monitor Compute Savings Plans coverage and receive notifications is to create a daily budget using AWS Budgets (Option A). AWS Budgets can be set up with alerts that trigger when the budgeted amount for Compute Savings Plans falls below a specified threshold, ensuring that the company is notified promptly if usage drops. This approach requires minimal ongoing effort and leverages AWS's built-in budgeting and alerting capabilities.

Creating a Lambda function for reporting (Option B) would require additional development and maintenance. A daily AWS Budgets report (Option C) would not automatically send notifications. While a Savings Plans alert subscription (Option D) could work, it is less flexible and does not provide the same level of detail as a budget alert.

解析: The most operationally efficient solution to monitor Compute Savings Plans coverage and receive notifications is to create a daily budget using AWS Budgets (Option A). AWS Budgets can be set up with alerts that trigger when the budgeted amount for Compute Savings Plans falls below a specified threshold, ensuring that the company is notified promptly if usage drops. This approach requires minimal ongoing effort and leverages AWS's built-in budgeting and alerting capabilities.

Creating a Lambda function for reporting (Option B) would require additional development and maintenance. A daily AWS Budgets report (Option C) would not automatically send notifications. While a Savings Plans alert subscription (Option D) could work, it is less flexible and does not provide the same level of detail as a budget alert.

616. #Question #716A 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?

- 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.

答案：A

解析：To make the Amazon MSK cluster publicly available and ensure data encryption with the most operational efficiency, the architect should configure public subnets within the existing VPC (Option A) and deploy the MSK cluster in those public subnets. Updating the MSK cluster security settings to enable mutual TLS authentication will provide the necessary encryption for data in transit. Creating a new VPC (Option B) would add unnecessary complexity and overhead. Deploying an ALB (Option C) or NLB (Option D) would not be as efficient because MSK can handle load balancing internally, and an additional load balancer would not contribute to encryption of the data in transit.

解析：To make the Amazon MSK cluster publicly available and ensure data encryption with the most operational efficiency, the architect should configure public subnets within the existing VPC (Option A) and deploy the MSK cluster in those public subnets. Updating the MSK cluster security settings to enable mutual TLS authentication will provide the necessary encryption for data in transit. Creating a new VPC (Option B) would add unnecessary complexity and overhead. Deploying an ALB (Option C) or NLB (Option D) would not be as efficient because MSK can handle

load balancing internally, and an additional load balancer would not contribute to encryption of the data in transit.

617. #Question #717A 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?

- 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.

答案: D

解析: To migrate the legacy application to AWS while maintaining security, resilience, and immediate processing of order files from the ERP system, the company should create an AWS Transfer Family SFTP

internal server (Option D). This setup ensures secure file transfer within the AWS environment and supports the required SFTP protocol. Using Amazon S3 storage is appropriate for durability and scalability. An AWS Lambda function can be used to process the order files, and a Transfer Family managed workflow can be set up to invoke the Lambda function, ensuring that the processing occurs immediately upon file upload.

解析: To migrate the legacy application to AWS while maintaining security, resilience, and immediate processing of order files from the ERP system, the company should create an AWS Transfer Family SFTP internal server (Option D). This setup ensures secure file transfer within the AWS environment and supports the required SFTP protocol. Using Amazon S3 storage is appropriate for durability and scalability. An AWS Lambda function can be used to process the order files, and a Transfer Family managed workflow can be set up to invoke the Lambda function, ensuring that the processing occurs immediately upon file upload.

618. #Question #718A 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?

- 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.

答案: C

解析: To meet the requirement of keeping data processing on-premises while improving scalability and reducing operational complexity, the architect should migrate the Apache Hadoop and Apache Spark applications to Amazon EMR clusters on AWS Outposts (Option C). AWS Outposts allows running AWS services on-premises, which helps to maintain data processing within the company's data center. This approach leverages the scalability and management benefits of EMR without the need to move data over the network to a remote AWS location.

解析: To meet the requirement of keeping data processing on-premises while improving scalability and reducing operational complexity, the architect should migrate the Apache Hadoop and Apache Spark applications to Amazon EMR clusters on AWS Outposts (Option C). AWS Outposts allows running AWS services on-premises, which helps to maintain data processing within the company's data center. This approach leverages the scalability and management benefits of EMR without the need to move data over the network to a remote AWS location.

619. #Question #719A 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?

- 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.

答案: B

解析: To host the data with the least operational overhead, the company should create an Amazon FSx for ONTAP instance (Option B). FSx for ONTAP supports both SMB and NFS protocols, which aligns with the requirements for EC2 instances to access the data. The auto tiering policy will automatically move infrequently accessed data to a more cost-effective storage tier, while still keeping the frequently accessed data readily available. This solution provides a balance between performance and cost, with minimal overhead for managing data tiers.

解析: To host the data with the least operational overhead, the company should create an Amazon FSx for ONTAP instance (Option B). FSx for ONTAP supports both SMB and NFS protocols, which aligns with the requirements for EC2 instances to access the data. The auto tiering policy will automatically move infrequently accessed data to a more cost-effective storage tier, while still keeping the frequently accessed data readily available. This solution provides a balance between performance and cost, with minimal overhead for managing data tiers.

620. #Question #720A 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?

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.

答案: C

解析: To minimize downtime and allow for a scalable, flexible, and maintainable application architecture, the company should run the application on Amazon ECS as microservices (Option C). ECS supports service auto scaling, which can adjust the number of instances based on demand, and it allows for running containerized applications as microservices. This approach enables independent updating and scaling of each component of the application, reducing downtime during updates and providing a more resilient architecture.

解析: To minimize downtime and allow for a scalable, flexible, and maintainable application architecture, the company should run the application on Amazon ECS as microservices (Option C). ECS supports service auto scaling, which can adjust the number of instances based on demand, and it allows for running containerized applications as microservices. This approach enables independent updating and scaling of each component of the application, reducing downtime during updates and providing a more resilient architecture.

621. #Question #721A 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?

- 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.

答案: D

解析: To meet the requirements of a serverless microservices architecture that supports Python, scales automatically, and requires minimal infrastructure and operational support, the company should use AWS Lambda (Option D). Lambda allows developers to run code without provisioning or managing servers, and it automatically scales with the number of requests. This serverless solution is well-suited for handling variable loads and is cost-effective for high-request components.

解析: To meet the requirements of a serverless microservices architecture that supports Python, scales automatically, and requires minimal infrastructure and operational support, the company should use AWS Lambda (Option D). Lambda allows developers to run code without provisioning or managing servers, and it automatically scales with the number of requests. This serverless solution is well-suited for handling variable loads and is cost-effective for high-request components.

622. #Question #722A 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?

- 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 peering connections 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.

答案：A

解析：To centrally manage the networking architecture with the least operational overhead, the company should create a transit gateway (Option A). The transit gateway can be connected to the existing Direct Connect connection and used to associate with all VPCs, enabling them to communicate with each other and the on-premises network without the need for complex peering or VPN setups. The route propagation feature of the transit gateway ensures that routes between the VPCs are automatically advertised, simplifying network management.

解析：To centrally manage the networking architecture with the least operational overhead, the company should create a transit gateway (Option A). The transit gateway can be connected to the existing Direct Connect connection and used to associate with all VPCs, enabling them to communicate with each other and the on-premises network without the need for complex peering or VPN setups. The route propagation feature of the transit gateway ensures that routes between the VPCs are automatically advertised, simplifying network management.

623. #Question #723A 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?

- 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.

答案：C

解析：To patch EC2 instances without disrupting the running applications, the company can enable Default Host Configuration Management in AWS Systems Manager (Option C). This feature allows Systems Manager to manage patching and updates for the EC2 instances, including those connected to Amazon RDS databases. It does not require the creation of a new IAM role or user, nor does it require modifying the existing IAM role's policies.

解析：To patch EC2 instances without disrupting the running applications, the company can enable Default Host Configuration Management in AWS Systems Manager (Option C). This feature allows Systems Manager to manage patching and updates for the EC2 instances, including those connected to Amazon RDS databases. It does not require the creation of a new IAM role or user, nor does it require modifying the existing IAM role's policies.

624. #Question #724A 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?

- 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.

答案：B

解析：To resolve the issue with the least administrative overhead, the solutions architect should use the Kubernetes Cluster Autoscaler (Option B). The Cluster Autoscaler is designed to automatically adjust the number of nodes in an EKS cluster based on the workload, ensuring that the cluster has the necessary resources to handle the current demand without manual intervention.

解析：To resolve the issue with the least administrative overhead, the solutions architect should use the Kubernetes Cluster Autoscaler (Option B). The Cluster Autoscaler is designed to automatically adjust the number of nodes in an EKS cluster based on the workload, ensuring that the cluster has the necessary resources to handle the current demand without manual intervention.

625. #Question #725A 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?

- 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.

答案：B

解析：To reduce the increasing S3 storage costs, the solutions architect should enable an S3 Lifecycle policy that deletes incomplete multipart uploads (Option B). Since the objects are frequently replaced and multipart uploads can incur additional costs if they are not completed, a lifecycle policy can help manage and reduce these costs by automatically cleaning up incomplete uploads. This approach directly addresses the

issue of increasing costs without affecting the availability of the objects that are successfully uploaded.

解析: To reduce the increasing S3 storage costs, the solutions architect should enable an S3 Lifecycle policy that deletes incomplete multipart uploads (Option B). Since the objects are frequently replaced and multipart uploads can incur additional costs if they are not completed, a lifecycle policy can help manage and reduce these costs by automatically cleaning up incomplete uploads. This approach directly addresses the issue of increasing costs without affecting the availability of the objects that are successfully uploaded.

626. #Question #726A 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?

- 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.

答案: D

解析: To improve the performance of the data tier for the multiplayer game, the solutions architect should deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance (Option D). By using Redis as a caching layer, the game can offload frequent read operations from the PostgreSQL database, thereby reducing the load on the database.

and improving response times for location tracking. This approach is particularly effective for read-heavy workloads and can significantly enhance performance during peak usage periods.

解析: To improve the performance of the data tier for the multiplayer game, the solutions architect should deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance (Option D). By using Redis as a caching layer, the game can offload frequent read operations from the PostgreSQL database, thereby reducing the load on the database and improving response times for location tracking. This approach is particularly effective for read-heavy workloads and can significantly enhance performance during peak usage periods.

627. #Question #727A 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**?

- 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.

答案: C

解析: To prevent accidental deletion of DynamoDB tables with the least operational overhead, the company should configure deletion protection on the DynamoDB tables (Option C). Deletion protection is a simple yet effective feature that prevents tables from being deleted without explicit administrator action, thus reducing the risk of data loss due to accidental deletions. This approach requires minimal configuration and does not involve the complexity of setting up automated backups or recovery processes.

解析: To prevent accidental deletion of DynamoDB tables with the least operational overhead, the company should configure deletion protection on the DynamoDB tables (Option C). Deletion protection is a simple yet effective feature that prevents tables from being deleted without explicit administrator action, thus reducing the risk of data loss due to accidental deletions. This approach requires minimal configuration and does not involve the complexity of setting up automated backups or recovery processes.

628. #Question #728A 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?

- 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.

答案: C

解析: To migrate the storage infrastructure to AWS with immediate data retrieval and no additional cost, the company should deploy AWS Storage Gateway using stored volumes (Option C). **Stored volumes keep the entire dataset on-premises while asynchronously backing up snapshots to Amazon S3.** This allows for low-latency local access to the data and cost-effective, durable storage in the cloud. This solution minimizes bandwidth costs as it does not require data to be transferred over the

network for immediate access.

解析: To migrate the storage infrastructure to AWS with immediate data retrieval and no additional cost, the company should deploy AWS Storage Gateway using stored volumes (Option C). Stored volumes keep the entire dataset on-premises while asynchronously backing up snapshots to Amazon S3. This allows for low-latency local access to the data and cost-effective, durable storage in the cloud. This solution minimizes bandwidth costs as it does not require data to be transferred over the network for immediate access.

629. #Question #729A 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?

- 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.

答案: B

解析: To create an automated scaling plan that considers both historical workload trends and live changes in utilization, the solutions architect should recommend enabling predictive scaling (Option B). Predictive scaling uses machine learning to forecast demand and adjust the number of resources accordingly. By configuring dynamic scaling with target tracking, the company can ensure that the scaling plan automatically adjusts to maintain the desired performance levels based on the forecast

and real-time data.

解析: To create an automated scaling plan that considers both historical workload trends and live changes in utilization, the solutions architect should recommend enabling predictive scaling (Option B). Predictive scaling uses machine learning to forecast demand and adjust the number of resources accordingly. By configuring dynamic scaling with target tracking, the company can ensure that the scaling plan automatically adjusts to maintain the desired performance levels based on the forecast and real-time data.

630. #Question #730A 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?**

- 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.

答案: A

解析: To cost-effectively alleviate the effect of repeated reads on the DB cluster, the company should implement an Amazon ElastiCache for Redis cluster (Option A). By caching the results of the repeated read statements in Redis, the load on the DB cluster can be significantly reduced, as these common queries are served from the cache rather than the database. This approach is more cost-effective than adding additional read replicas (Option B) or configuring Auto Scaling for read replicas (Option C), as it offloads the repeated reads without the need for

additional database resources.

解析: To cost-effectively alleviate the effect of repeated reads on the DB cluster, the company should implement an Amazon ElastiCache for Redis cluster (Option A). By caching the results of the repeated read statements in Redis, the load on the DB cluster can be significantly reduced, as these common queries are served from the cache rather than the database. This approach is more cost-effective than adding additional read replicas (Option B) or configuring Auto Scaling for read replicas (Option C), as it offloads the repeated reads without the need for additional database resources.

631. #Question #731A 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?

- 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.

答案: C

解析: Since the issue is with requests not returning the latest data, the solutions architect should recommend requesting strongly consistent reads for the table (Option C). DynamoDB provides two types of reads: eventually consistent reads (default) and strongly consistent reads. Strongly consistent reads ensure that the response includes the most recent data, reflecting all writes that received a successful response before the read. This change would help in retrieving the latest data without impacting the performance or latency, which are already acceptable.

解析: Since the issue is with requests not returning the latest data, the solutions architect should recommend requesting strongly consistent reads for the table (Option C). DynamoDB provides two types of reads:

eventually consistent reads (default) and strongly consistent reads. Strongly consistent reads ensure that the response includes the most recent data, reflecting all writes that received a successful response before the read. This change would help in retrieving the latest data without impacting the performance or latency, which are already acceptable.

632. #Question #732A 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?

- 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.

答案：B

解析：To protect the application and database from SQL injection and other web-based attacks with the least operational overhead, the company should use AWS WAF (Option B). AWS WAF can be configured to filter and block malicious traffic before it reaches the application and database, providing a layer of security against common web exploits. Additionally, using RDS parameter groups allows for the management of database security settings in a centralized manner. This approach is more efficient than manually configuring security groups and network ACLs (Option A), using AWS Network Firewall (Option C), or managing database accounts and privileges (Option D).

解析：To protect the application and database from SQL injection and other web-based attacks with the least operational overhead, the company should use AWS WAF (Option B). AWS WAF can be configured to filter and

block malicious traffic before it reaches the application and database, providing a layer of security against common web exploits. Additionally, using RDS parameter groups allows for the management of database security settings in a centralized manner. This approach is more efficient than manually configuring security groups and network ACLs (Option A), using AWS Network Firewall (Option C), or managing database accounts and privileges (Option D).

633. #Question #733An 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?

- 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.

答案: B

解析: To most operationally efficiently prevent malicious activity and identify abnormal login attempts, the company should enable the Amazon RDS Protection feature in Amazon GuardDuty (Option B). GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior, including unusual login attempts. Enabling RDS Protection provides an additional layer of security specifically for RDS instances. This approach is more focused and efficient than using SCPs (Option A), which are more about permissions and do not detect malicious activity, or manually managing logs and events (Options C and D).

解析: To most operationally efficiently prevent malicious activity and identify abnormal login attempts, the company should enable the Amazon RDS Protection feature in Amazon GuardDuty (Option B). GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior, including unusual login attempts. Enabling RDS Protection provides an additional layer of security specifically for RDS instances. This approach is more focused and efficient than using SCPs (Option A), which are more about permissions and do not detect malicious activity, or manually managing logs and events (Options C and D).

634. #Question #734A 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?

- 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.

答案: D

解析: To meet the requirements for scalable connectivity between Regions and data centers with reduced operational overhead, the solutions architect should connect the existing Direct Connect connection to a

Direct Connect gateway (Option D). By using the Direct Connect gateway, the company can establish a single, centralized connection that routes traffic between the VPCs in different Regions and the on-premises data centers. This approach is more scalable and requires less overhead than setting up inter-Region VPC peering (Option A), creating private virtual interfaces (Option B), or managing a complex VPN network (Option C).

解析: To meet the requirements for scalable connectivity between Regions and data centers with reduced operational overhead, the solutions architect should connect the existing Direct Connect connection to a Direct Connect gateway (Option D). By using the Direct Connect gateway, the company can establish a single, centralized connection that routes traffic between the VPCs in different Regions and the on-premises data centers. This approach is more scalable and requires less overhead than setting up inter-Region VPC peering (Option A), creating private virtual interfaces (Option B), or managing a complex VPN network (Option C).

635. #Question #735A 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?

- 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.

答案：A

解析：To handle large traffic spikes and process updates in order while minimizing management overhead, the solutions architect should use Amazon Kinesis Data Streams (Option A). Kinesis Data Streams can handle high-throughput, real-time data streaming, and can be combined with AWS Lambda for serverless processing of the data. Storing the processed updates in Amazon DynamoDB ensures a highly available and scalable database. This solution is more cost-effective and requires less management overhead compared to managing a fleet of EC2 instances (Option B), using SNS and SQS which may introduce additional complexity (Option C and D), or storing data in a SQL database on EC2 (Option C), which would require more operational management.

解析：To handle large traffic spikes and process updates in order while minimizing management overhead, the solutions architect should use Amazon Kinesis Data Streams (Option A). Kinesis Data Streams can handle high-throughput, real-time data streaming, and can be combined with AWS Lambda for serverless processing of the data. Storing the processed updates in Amazon DynamoDB ensures a highly available and scalable database. This solution is more cost-effective and requires less management overhead compared to managing a fleet of EC2 instances (Option B), using SNS and SQS which may introduce additional complexity (Option C and D), or storing data in a SQL database on EC2 (Option C), which would require more operational management.

636. #Question #736A 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?

- 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.

答案: B

解析: The most cost-effective solution for creating a centralized log analysis system without incurring additional operational overhead or leaving the us-west-2 Region is to use S3 Same-Region Replication (Option B). This feature allows for the replication of logs from multiple source S3 buckets to a single destination S3 bucket within the same region. This method is more efficient than manually creating a lifecycle policy (Option A), writing a custom script (Option C), or using AWS Lambda functions (Option D), which would require additional setup and ongoing maintenance.

解析: The most cost-effective solution for creating a centralized log analysis system without incurring additional operational overhead or leaving the us-west-2 Region is to use S3 Same-Region Replication (Option B). This feature allows for the replication of logs from multiple source S3 buckets to a single destination S3 bucket within the same region. This method is more efficient than manually creating a lifecycle policy (Option A), writing a custom script (Option C), or using AWS Lambda functions (Option D), which would require additional setup and ongoing maintenance.

637. #Question #738A 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?**

- 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.

答案：B

解析：To optimize the user experience and provide the lowest latency for content uploads, the company should use S3 Transfer Acceleration (Option B). S3 Transfer Acceleration is designed to speed up the upload process by using Amazon's global network to create an optimized path for the upload. This feature is particularly beneficial for users who are far from the S3 bucket's location, as it reduces the time it takes to transfer files to Amazon S3. Using Amazon CloudFront (Option A) or EC2 instances (Option C) would not be as efficient for uploads, and while using multiple CloudFront distributions (Option D) can improve content delivery, it does not address the upload latency issue.

解析：To optimize the user experience and provide the lowest latency for content uploads, the company should use S3 Transfer Acceleration (Option B). S3 Transfer Acceleration is designed to speed up the upload process by using Amazon's global network to create an optimized path for the upload. This feature is particularly beneficial for users who are far from the S3 bucket's location, as it reduces the time it takes to transfer files to Amazon S3. Using Amazon CloudFront (Option A) or EC2 instances (Option C) would not be as efficient for uploads, and while using multiple CloudFront distributions (Option D) can improve content

delivery, it does not address the upload latency issue.

638. #Question #739A 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?

- 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.

答案：B

解析：To meet the requirements with the least operational overhead, the company should send the requests from the API Gateway REST API to Amazon EventBridge (Option B). EventBridge is a serverless event bus that can trigger target Lambda functions in response to incoming events, without the need for additional components like SNS or SQS. This approach simplifies the architecture and reduces operational overhead compared to managing message queues or using a messaging system like Amazon MSK.

解析：To meet the requirements with the least operational overhead, the company should send the requests from the API Gateway REST API to Amazon EventBridge (Option B). EventBridge is a serverless event bus that can

trigger target Lambda functions in response to incoming events, without the need for additional components like SNS or SQS. This approach simplifies the architecture and reduces operational overhead compared to managing message queues or using a messaging system like Amazon MSK.

639. #Question #740A 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?

- 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).

答案: A

解析: To encrypt both existing and future unencrypted objects in Amazon S3 with a customer-provided key, the solutions architect should use Amazon S3 Inventory to create a list of unencrypted objects (Option A). Then, an S3 Batch Operations job can be configured to encrypt these objects with SSE-C. Additionally, the S3 default encryption feature should be set to use SSE-C to ensure that all future objects are

encrypted with the customer-provided key. This approach addresses both the encryption of current unencrypted objects and sets a default encryption for new objects.

解析: To encrypt both existing and future unencrypted objects in Amazon S3 with a customer-provided key, the solutions architect should use Amazon S3 Inventory to create a list of unencrypted objects (Option A). Then, an S3 Batch Operations job can be configured to encrypt these objects with SSE-C. Additionally, the S3 default encryption feature should be set to use SSE-C to ensure that all future objects are encrypted with the customer-provided key. This approach addresses both the encryption of current unencrypted objects and sets a default encryption for new objects.

640. #Question #741The 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?**

- 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. By creating 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.

答案: A

解析: To rapidly migrate the DNS hosting service to a more resilient managed DNS service on AWS, the solutions architect should create an

Amazon Route 53 public hosted zone (Option A). This will allow the company to import the existing domain records from the previous provider and ensure high availability and reliability for the DNS service. A public hosted zone is appropriate for domains that are accessible over the internet. Creating a private hosted zone (Option B) would be suitable for internal, private DNS names within a VPC, which is not the requirement in this scenario. Options C and D do not directly address the need for a rapid migration to a managed DNS service.

解析: To rapidly migrate the DNS hosting service to a more resilient managed DNS service on AWS, the solutions architect should create an Amazon Route 53 public hosted zone (Option A). This will allow the company to import the existing domain records from the previous provider and ensure high availability and reliability for the DNS service. A public hosted zone is appropriate for domains that are accessible over the internet. Creating a private hosted zone (Option B) would be suitable for internal, private DNS names within a VPC, which is not the requirement in this scenario. Options C and D do not directly address the need for a rapid migration to a managed DNS service.

641. #Question #742A 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?

- 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.

答案：A

解析：To meet the requirements with the least administrative overhead, the company should use AWS AppConfig (Option A) to manage the application configuration and AWS Secrets Manager for securely storing and retrieving database credentials and other secrets. This approach provides a centralized and secure way to manage configurations and credentials without the need for additional scripting or custom solutions. Using AWS Lambda (Option B) or an encrypted S3 file (Option C) would require more management and potentially more complex access controls. Using Amazon RDS (Option D) to store credentials is not a recommended practice as it is not designed for secret management.

解析：To meet the requirements with the least administrative overhead, the company should use AWS AppConfig (Option A) to manage the application configuration and AWS Secrets Manager for securely storing and retrieving database credentials and other secrets. This approach provides a centralized and secure way to manage configurations and credentials without the need for additional scripting or custom solutions. Using AWS Lambda (Option B) or an encrypted S3 file (Option C) would require more management and potentially more complex access controls. Using Amazon RDS (Option D) to store credentials is not a recommended practice as it is not designed for secret management.

642. #Question #743 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?

- 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.

答案: D

解析: To satisfy the security requirements for encrypting data in transit, the solutions architect should download AWS-provided root certificates (Option D) and use them for all connections to the RDS instance. This ensures that the data is encrypted during transmission between the application and the database. Enabling IAM database authentication (Option A) is more about user authentication and not about data encryption. Using self-signed certificates (Option B) is not recommended for production environments as they are not trusted by clients by default. Taking a snapshot and restoring it with encryption enabled (Option C) addresses encryption at rest, not in transit.

解析: To satisfy the security requirements for encrypting data in transit, the solutions architect should download AWS-provided root certificates (Option D) and use them for all connections to the RDS instance. This ensures that the data is encrypted during transmission between the application and the database. Enabling IAM database authentication (Option A) is more about user authentication and not about data encryption. Using self-signed certificates (Option B) is not recommended for production environments as they are not trusted by clients by default. Taking a snapshot and restoring it with encryption enabled (Option C) addresses encryption at rest, not in transit.

643. #Question #744A 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?

- 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.

答案：A

解析：A. A Network Load Balancer with an associated Elastic IP address.

解析：Network Load Balancer (NLB) 允许您分配一个或多个 Elastic IP addresses (EIPs)。NLB 会将传入的流量分发到多个目标，例如 EC2 实例、容器和 IP 地址等。对于需要固定 IP

地址以便允许防火墙配置的场景，此选项是可行的。NLB 还可以处理 TCP、UDP 和 TLS 流量，提供了更高的灵活性。B. An Application Load Balancer with an associated Elastic IP address.

解析：Application Load Balancer (ALB)

主要是用于 HTTP/HTTPS 流量。然而，ALB 本身不支持直接与 Elastic IP

地址关联。它使用动态分配的 DNS 名称，这不适合需要固定 IP

地址以配置防火墙的客户。C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.

解析：虽然 Amazon Route 53 可以用来为 Elastic IP 地址创建一个 A

记录，但这并不能解决负载均衡的问题。此选项只是为单个 Elastic IP

地址提供了一个 DNS 名称，而不提供负载均衡功能。D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

解析：虽然这种方法理论上可以工作，但它引入了一个单点故障（即该 EC2 实例），并且需要额外的管理和维护工作。此外，这种方法可能不如直接使用支持 Elastic IP 的负载均衡器高效或可靠。参考答案：

考虑到客户需要通过防火墙允许特定的 IP

地址，并且需要一个负载均衡解决方案，选项 A（带有相关 Elastic IP 地址的网络负载均衡器）是最合适的选择。它提供了负载均衡功能，同时允许使用固定的 Elastic IP 地址，从而满足了客户的需求。因此，正确答案应该是 A. A Network Load Balancer with an associated Elastic IP address.

解析：A. A Network Load Balancer with an associated Elastic IP address.

解析：Network Load Balancer (NLB) 允许您分配一个或多个 Elastic IP addresses (EIPs)。NLB 会将传入的流量分发到多个目标，例如 EC2 实例、容器和 IP 地址等。对于需要固定 IP

地址以便允许防火墙配置的场景，此选项是可行的。NLB 还可以处理 TCP、UDP 和 TLS 流量，提供了更高的灵活性。B. An Application Load Balancer with an associated Elastic IP address.

解析：Application Load Balancer (ALB)

主要是用于 HTTP/HTTPS 流量。然而，ALB 本身不支持直接与 Elastic IP

地址关联。它使用动态分配的 DNS 名称，这不适合需要固定 IP 地址以配置防火墙的客户。C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address. 解析：虽然 Amazon Route 53 可以用来为 Elastic IP 地址创建一个 A

记录，但这并不能解决负载均衡的问题。此选项只是为单个 Elastic IP 地址提供了一个 DNS 名称，而不提供负载均衡功能。D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

解析：虽然这种方法理论上可以工作，但它引入了一个单点故障（即该 EC2 实例），并且需要额外的管理和维护工作。此外，这种方法可能不如直接使用支持 Elastic IP 的负载均衡器高效或可靠。参考答案：

考虑到客户需要通过防火墙允许特定的 IP

地址，并且需要一个负载均衡解决方案，选项 A（带有相关 Elastic IP 地址的网络负载均衡器）是最合适的选择。它提供了负载均衡功能，同时允许使用固定的 Elastic IP 地址，从而满足了客户的需求。因此，正确答案应该是 A. A Network Load Balancer with an associated Elastic IP address.

644. #Question #745A 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?

- 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.

答案：B

解析：The correct answer to secure the root user in a newly established AWS account is: B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user. Here's why this is the recommended approach and some additional best practices for securing

the root user:

- 1. Create IAM users for daily administrative tasks:
- This follows the principle of least privilege by using separate accounts with appropriate permissions for day-to-day operations.
- It reduces the risk of accidental changes or unauthorized access to critical account settings.
- 2. Enable multi-factor authentication (MFA) on the root user:
 - MFA adds an extra layer of security by requiring a second form of authentication in addition to the password.
 - This significantly reduces the risk of unauthorized access, even if the password is compromised.
- Additional best practices for securing the root user:

 - 3. Use a strong, unique password for the root user account.
 - 4. Avoid creating access keys for the root user.
 - 5. Store root user credentials securely and limit access to them.
 - 6. Use the root user only for tasks that specifically require root user access.
 - 7. Regularly review and update the contact information associated with the root user account.
 - 8. Set up AWS CloudTrail to monitor and log root user activity.
 - 9. Consider using AWS Organizations to manage multiple accounts and implement service control policies (SCPs) to restrict root user actions.
 - 10. Periodically review and test the process for accessing the root user account to ensure it's functioning correctly.

解析: The correct answer to secure the root user in a newly established AWS account is: B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user. Here's why this is the recommended approach and some additional best practices for securing

the root user:

- 1. Create IAM users for daily administrative tasks:
 - This follows the principle of least privilege by using separate accounts with appropriate permissions for day-to-day operations.
 - It reduces the risk of accidental changes or unauthorized access to critical account settings.
- 2. Enable multi-factor authentication (MFA) on the root user:
 - MFA adds an extra layer of security by requiring a second form of authentication in addition to the password.
 - This significantly reduces the risk of unauthorized access, even if the password is compromised.
- Additional best practices for securing the root user:

 - 3. Use a strong, unique password for the root user account.
 - 4. Avoid creating access keys for the root user.
 - 5. Store root user credentials securely and limit access to them.
 - 6. Use the root user only for tasks that specifically require root user access.
 - 7. Regularly review and update the contact information associated with the root user account.
 - 8. Set up AWS CloudTrail to monitor and log root user activity.
 - 9. Consider using AWS Organizations to manage multiple accounts and implement service control policies (SCPs) to restrict root user actions.
 - 10. Periodically review and test the process for accessing the root user account to ensure it's functioning correctly.

Remember, the goal is to minimize the use of the root user while ensuring it remains secure for the rare occasions when it's needed. By implementing these practices, you can significantly enhance the security of your AWS account.

Sources

 - [1] [SEC01-BP02 Secure account root user and properties – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2023-10-03/framework/sec_securely_operate_aws_account.html)
 - [3] [SEC01-BP02 Secure account root user and properties – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2024-06-27/framework/sec_securely_operate_aws_account.html)
 - [6] [SEC01-BP02 Secure account root user and properties – Security Pillar] (https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_securely_operate_aws_account.html)

645. #Question #747A 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?

- 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.

答案：C

解析：To migrate the data with the least operational overhead, the solutions architect should use AWS DataSync to migrate the data to Amazon FSx for Windows File Server (Option C). This solution allows the company to maintain the existing SMB-based access to the data, which is critical since the company does not want to change its applications. FSx for Windows File Server is designed to provide a scalable, high-performance file system that is fully compatible with Windows-based applications, making it a suitable choice for the migration.

解析：To migrate the data with the least operational overhead, the solutions architect should use AWS DataSync to migrate the data to Amazon FSx for Windows File Server (Option C). This solution allows the company to maintain the existing SMB-based access to the data, which is critical since the company does not want to change its applications. FSx for Windows File Server is designed to provide a scalable, high-performance file system that is fully compatible with Windows-based applications, making it a suitable choice for the migration.

646. #Question #748A 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?

- 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 user to the new IAM policy.
- 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.

答案：A

解析：To enable the monitoring account to query and visualize observability data across all other accounts in the organization, the company should enable CloudWatch cross-account observability (Option A).

This feature allows one account to collect and view data from other accounts. Deploying an AWS CloudFormation template in each account, as provided by the monitoring account, streamlines the process of setting up the necessary permissions and sharing configurations.

解析：To enable the monitoring account to query and visualize observability data across all other accounts in the organization, the company should enable CloudWatch cross-account observability (Option A). This feature allows one account to collect and view data from other accounts. Deploying an AWS CloudFormation template in each account, as provided by the monitoring account, streamlines the process of setting up the necessary permissions and sharing configurations.

647. #Question #749A 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?

- 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.

答案：B

解析：To protect the application from the external malicious IP, the solutions architect should modify the configuration of AWS WAF (Option B) to include an IP match condition that blocks the specified IP address. AWS WAF is designed to filter and block malicious traffic, making it the appropriate tool for this task. Modifying the network ACL on the CloudFront distribution (Option A) or the EC2 instances (Option C) would not be effective since CloudFront does not have network ACLs, and direct access to EC2 instances is not the point of entry for the web traffic. Modifying the security groups for the EC2 instances (Option D) would also not block traffic that has already passed through the ALB.

解析：To protect the application from the external malicious IP, the solutions architect should modify the configuration of AWS WAF (Option B) to include an IP match condition that blocks the specified IP address. AWS WAF is designed to filter and block malicious traffic, making it the appropriate tool for this task. Modifying the network ACL on the CloudFront distribution (Option A) or the EC2 instances (Option C) would not be effective since CloudFront does not have network ACLs, and direct access to EC2 instances is not the point of entry for the web traffic. Modifying the security groups for the EC2 instances (Option D) would also not block traffic that has already passed through the ALB.

648. #Question #750A 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?

- 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.

答案：C

解析：To provide access to several thousand employees using an existing identity provider, the solutions architect should configure AWS IAM Identity Center (AWS SSO) (Option C). AWS SSO allows for the integration with an existing IdP, enabling the company to provision users and groups from the IdP for access to multiple AWS accounts without the need to create IAM users in each account. This approach simplifies user management and is more scalable than creating individual IAM users (Option A) or root users (Option B). AWS RAM (Option D) is used for resource sharing rather than user authentication.

解析：To provide access to several thousand employees using an existing identity provider, the solutions architect should configure AWS IAM Identity Center (AWS SSO) (Option C). AWS SSO allows for the integration with an existing IdP, enabling the company to provision users and groups from the IdP for access to multiple AWS accounts without the need to create IAM users in each account. This approach simplifies user management and is more scalable than creating individual IAM users (Option A) or root users (Option B). AWS RAM (Option D) is used for

resource sharing rather than user authentication.

649. #Question #751A 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?

- 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.

答案：C

解析：To grant full access to AWS services and resources, the solutions architect should attach the **AdministratorAccess identity-based policy** (Option C) to the IAM user group. **This policy provides full access to all AWS services and resources.** Placing each of the five designated employee IAM users in the IAM user group with this policy attached will ensure they have the necessary permissions. The correct choice is an identity-based policy because it is directly associated with the user or group, ensuring that all users in the group inherit the permissions defined in the policy.

解析：To grant full access to AWS services and resources, the solutions architect should attach the AdministratorAccess identity-based policy (Option C) to the IAM user group. This policy provides full access to all AWS services and resources. Placing each of the five designated employee

IAM users in the IAM user group with this policy attached will ensure they have the necessary permissions. The correct choice is an identity-based policy because it is directly associated with the user or group, ensuring that all users in the group inherit the permissions defined in the policy.

650. #Question #753A 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?

- 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.

答案: D

解析: Option D provides a highly available and resilient solution by leveraging AWS Transfer for SFTP and Amazon S3, which are designed to be durable and available. The use of Amazon S3 for storage ensures that the data is redundantly stored across multiple Availability Zones. Additionally, by using an EC2 instance in an Auto Scaling group with a scheduled scaling policy, the solution can handle the batch processing workload efficiently while minimizing operational effort.

解析: Option D provides a highly available and resilient solution by leveraging AWS Transfer for SFTP and Amazon S3, which are designed to be durable and available. The use of Amazon S3 for storage ensures that the data is redundantly stored across multiple Availability Zones. Additionally, by using an EC2 instance in an Auto Scaling group with a scheduled scaling policy, the solution can handle the batch processing workload efficiently while minimizing operational effort.

651. #Question #754A 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?

- 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.

答案: B

解析: To improve the availability and performance of the HTTP-based application for global users, an Application Load Balancer (ALB) should be used, which is suitable for HTTP and HTTPS applications (Option B). ALBs can distribute traffic across multiple EC2 instances and support AWS

WAF for protection against web exploits. By deploying AWS WAF on the ALBs, the application is secured at the application layer. Furthermore, AWS Global Accelerator can be used in conjunction with ALBs to improve performance by routing users to the nearest AWS Region, and it provides static IP addresses as required.

解析: To improve the availability and performance of the HTTP-based application for global users, an Application Load Balancer (ALB) should be used, which is suitable for HTTP and HTTPS applications (Option B). ALBs can distribute traffic across multiple EC2 instances and support AWS WAF for protection against web exploits. By deploying AWS WAF on the ALBs, the application is secured at the application layer. Furthermore, AWS Global Accelerator can be used in conjunction with ALBs to improve performance by routing users to the nearest AWS Region, and it provides static IP addresses as required.

652. #Question #755A 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?

- 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.

答案: B

解析: To reduce the failover time when promoting a read replica to a primary writer in Amazon Aurora MySQL, using Amazon RDS Proxy (Option B) is the most appropriate solution. RDS Proxy can manage database connections efficiently and provide a performance boost by allowing multiple application instances to share database connections. This pooling of connections can also make the application more resilient to

database failures, as it can automatically connect to a standby DB instance while preserving application connections, thereby reducing the failover time.

解析: To reduce the failover time when promoting a read replica to a primary writer in Amazon Aurora MySQL, using Amazon RDS Proxy (Option B) is the most appropriate solution. RDS Proxy can manage database connections efficiently and provide a performance boost by allowing multiple application instances to share database connections. This pooling of connections can also make the application more resilient to database failures, as it can automatically connect to a standby DB instance while preserving application connections, thereby reducing the failover time.

653. #Question #756A 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**?

- 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.

答案：A

解析：To provide samples of conversations to an external service provider without sharing customer PII and to ensure the solution scales, an Object Lambda Access Point (Option A) can be used. This feature allows the creation of a Lambda function that processes and redacts PII directly when the files are accessed, ensuring that only non-sensitive data is provided to the external service provider. This approach has the least operational overhead as it does not require moving data, maintaining additional infrastructure, or manual redaction processes.

解析：To provide samples of conversations to an external service provider without sharing customer PII and to ensure the solution scales, an Object Lambda Access Point (Option A) can be used. This feature allows the creation of a Lambda function that processes and redacts PII directly when the files are accessed, ensuring that only non-sensitive data is provided to the external service provider. This approach has the least operational overhead as it does not require moving data, maintaining additional infrastructure, or manual redaction processes.

654. #Question #757A 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?

- 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.

答案：D

解析：To improve the recovery time for a legacy system running on a single EC2 instance without the ability to modify the application code, the architect should consider implementing storage redundancy (Option D). By using RAID configurations across two Amazon EBS volumes, the system can maintain data redundancy and help to minimize data loss in the event of a storage failure. This approach does not require changing the application or running multiple instances, making it a suitable solution for the given constraints.

解析：To improve the recovery time for a legacy system running on a single EC2 instance without the ability to modify the application code, the architect should consider implementing storage redundancy (Option D). By using RAID configurations across two Amazon EBS volumes, the system can maintain data redundancy and help to minimize data loss in the event of a storage failure. This approach does not require changing the application or running multiple instances, making it a suitable solution for the given constraints.

655. #Question #758A 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**?

- 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.

答案：A

解析：To deploy containerized applications with high availability across three Availability Zones with minimal operational overhead, Amazon Elastic Container Service (Option A) is the recommended solution. ECS can automatically spread tasks across multiple Availability Zones, ensuring high availability without significant changes to the application. By configuring ECS Service Auto Scaling with target tracking scaling and setting the task placement strategy to spread across Availability Zones, the company can achieve the desired operational efficiency.

解析：To deploy containerized applications with high availability across three Availability Zones with minimal operational overhead, Amazon Elastic Container Service (Option A) is the recommended solution. ECS can automatically spread tasks across multiple Availability Zones, ensuring high availability without significant changes to the application. By configuring ECS Service Auto Scaling with target tracking scaling and setting the task placement strategy to spread across Availability Zones, the company can achieve the desired operational efficiency.

656. #Question #759A 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?

- 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.

答案: C

解析: To ensure that the media company can provide streaming content within 5 minutes of a user purchase while minimizing costs, the solution involves storing newer movies in a more accessible storage class and older movies in a cheaper, yet retrievable, storage class. Option C is the most suitable as it uses S3 Intelligent-Tiering for newer movies, which automatically moves the data to the most cost-effective access tier without performance impact, and S3 Glacier Flexible Retrieval for older movies, which allows for expedited retrieval within minutes, thus meeting the requirement of rapid content delivery post-purchase.

解析: To ensure that the media company can provide streaming content within 5 minutes of a user purchase while minimizing costs, the solution involves storing newer movies in a more accessible storage class and older movies in a cheaper, yet retrievable, storage class. Option C is the most suitable as it uses S3 Intelligent-Tiering for newer movies, which automatically moves the data to the most cost-effective access tier without performance impact, and S3 Glacier Flexible Retrieval for older movies, which allows for expedited retrieval within minutes, thus meeting the requirement of rapid content delivery post-purchase.

657. #Question #760A 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?

- 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.

答案: C

解析: To meet the requirement of a serverless infrastructure capable of providing 50 GB of storage for a Docker container, the architect should choose the AWS Fargate launch type for Amazon ECS (Option C). Fargate is a serverless offering for Amazon ECS and Amazon EKS that allows users to run containers without managing the underlying infrastructure. By using Fargate with an Amazon EFS volume, the application can make use of persistent storage that is independent of the lifecycle of the container, thus meeting the storage needs with minimal operational overhead.

解析: To meet the requirement of a serverless infrastructure capable of providing 50 GB of storage for a Docker container, the architect should choose the AWS Fargate launch type for Amazon ECS (Option C). Fargate is a serverless offering for Amazon ECS and Amazon EKS that allows users to run containers without managing the underlying infrastructure. By using Fargate with an Amazon EFS volume, the application can make use of persistent storage that is independent of the lifecycle of the container, thus meeting the storage needs with minimal operational overhead.

658. #Question #761A 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?

- 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.

答案：D

解析：Since the company's LDAP directory service is not compatible with SAML, the solutions architect cannot use AWS IAM Identity Center, which relies on SAML for federation. Instead, the architect should develop a custom identity broker (Option D) that uses AWS STS to generate temporary security credentials. This approach allows the LDAP users to authenticate to AWS services without requiring direct integration between LDAP and AWS IAM.

解析：Since the company's LDAP directory service is not compatible with SAML, the solutions architect cannot use AWS IAM Identity Center, which relies on SAML for federation. Instead, the architect should develop a custom identity broker (Option D) that uses AWS STS to generate temporary security credentials. This approach allows the LDAP users to authenticate to AWS services without requiring direct integration between LDAP and AWS IAM.

659. #Question #762A 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?

- 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.

答案：C

解析：To protect against accidental deletion of AMIs with minimal operational overhead, the solutions architect should use the Recycle Bin feature (Option C). Recycle Bin is a service that protects your Amazon EC2 snapshots and AMIs from accidental deletion. By creating a retention rule within Recycle Bin, the company can ensure that deleted AMIs are retained for a specified period, allowing for easy recovery without the need for additional storage accounts or manual copying processes.

解析：To protect against accidental deletion of AMIs with minimal operational overhead, the solutions architect should use the Recycle Bin feature (Option C). Recycle Bin is a service that protects your Amazon EC2 snapshots and AMIs from accidental deletion. By creating a retention rule within Recycle Bin, the company can ensure that deleted AMIs are retained for a specified period, allowing for easy recovery without the need for additional storage accounts or manual copying processes.

660. #Question #763A 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?

- 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.

答案：B

解析：Given the large amount of data (150 TB) and the limited upload bandwidth (100 Mbps) available during nighttime, the most cost-effective and time-efficient solution for migrating the data to AWS within the

given deadline is to use multiple AWS Snowball devices (Option B). Snowball is a petabyte-scale data transport solution that uses physical storage devices to transfer large amounts of data into and out of AWS. This approach minimizes the time spent on data transfer and leverages the high bandwidth provided by AWS Snowball, thus meeting the migration deadline.

解析: Given the large amount of data (150 TB) and the limited upload bandwidth (100 Mbps) available during nighttime, the most cost-effective and time-efficient solution for migrating the data to AWS within the given deadline is to use multiple AWS Snowball devices (Option B). Snowball is a petabyte-scale data transport solution that uses physical storage devices to transfer large amounts of data into and out of AWS. This approach minimizes the time spent on data transfer and leverages the high bandwidth provided by AWS Snowball, thus meeting the migration deadline.

661. #Question #764A 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**?

- 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.

答案：B

解析：old (C) -->new(B) old: To achieve the goal of minimal operational overhead while enabling point-in-time recovery for the database, the best approach is to migrate the web and application tiers to Amazon EC2 instances, with the web tier in public subnets and the application tier in private subnets (Option C). For the database tier, migrating to Amazon RDS for MySQL allows the company to leverage RDS's built-in point-in-time recovery feature without the need for significant changes to the existing architecture. This solution also maintains security by keeping the application tier in private subnets.

解析：old (C) -->new(B) old: To achieve the goal of minimal operational overhead while enabling point-in-time recovery for the database, the best approach is to migrate the web and application tiers to Amazon EC2 instances, with the web tier in public subnets and the application tier in private subnets (Option C). For the database tier, migrating to Amazon RDS for MySQL allows the company to leverage RDS's built-in point-in-time recovery feature without the need for significant changes to the existing architecture. This solution also maintains security by keeping the application tier in private subnets.

662. #Question #765A 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?

- 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.

答案: C

解析: To grant another company's AWS account access to an SQS queue without requiring them to relinquish control over their own account permissions, the solutions architect should create an SQS access policy (Option C). This policy can be attached directly to the SQS queue and specifies the permissions that the other company's account will have, allowing them to poll the queue as needed while maintaining their account's security and permissions.

解析: To grant another company's AWS account access to an SQS queue without requiring them to relinquish control over their own account permissions, the solutions architect should create an SQS access policy (Option C). This policy can be attached directly to the SQS queue and specifies the permissions that the other company's account will have, allowing them to poll the queue as needed while maintaining their account's security and permissions.

663. #Question #766A 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?**

- 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.

答案：D

解析：For a secure and cost-effective solution to enable SSH access to EC2 instances, the solutions architect should utilize AWS Systems Manager Session Manager (Option D). This service allows developers to access their instances without needing to manage SSH keys or opening inbound SSH ports on the instances. By attaching the AmazonSSMManagedInstanceCore IAM policy to the EC2 instances, developers can connect to these instances through the AWS Systems Manager console, AWS CLI, or SDKs, which is a more secure and manageable approach compared to setting up VPNs or bastion hosts.

解析：For a secure and cost-effective solution to enable SSH access to EC2 instances, the solutions architect should utilize AWS Systems Manager Session Manager (Option D). This service allows developers to access their instances without needing to manage SSH keys or opening inbound SSH ports on the instances. By attaching the AmazonSSMManagedInstanceCore IAM policy to the EC2 instances, developers can connect to these instances through the AWS Systems Manager console, AWS CLI, or SDKs, which is a more secure and manageable approach compared to setting up VPNs or bastion hosts.

664. #Question #767A 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?

- 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.

答案：C

解析：Based on the pharmaceutical company's requirements, I recommend deploying an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage. This solution addresses the company's needs in the following ways: 1. Scalability: Amazon S3 provides virtually unlimited storage capacity, accommodating the company's exponentially growing data volume. 2. Cost-effectiveness: By migrating data to S3, the company can reduce ongoing capital expenses associated with on-premises storage arrays. 3. Immediate access to subset data: The file gateway caches frequently accessed data locally, ensuring that researchers can quickly access the subset of data they regularly need with minimal lag. 4. Hybrid storage solution: The file gateway acts as a bridge between on-premises systems and Amazon S3, allowing seamless integration with existing workflows and applications. 5. Data archiving: Less frequently accessed data can be automatically moved to lower-cost S3 storage tiers, further optimizing costs. To implement this solution: 1. Set up an Amazon S3 bucket to serve as the target storage. 2. Deploy and configure the AWS Storage Gateway file gateway appliance on-premises. 3. Migrate the existing data from the on-premises storage arrays to the file gateway. 4.

Configure caching policies to ensure frequently accessed data remains readily available.

5. Implement lifecycle policies in S3 to automatically move less frequently accessed data to lower-cost storage tiers. This approach provides a balance between immediate data access for researchers and cost-effective long-term storage for the entire dataset. It also allows for future scalability as the company's data continues to grow.

Remember to consult AWS documentation for the most up-to-date information on Storage Gateway and S3 capabilities, pricing, and best practices for your specific use case.

Sources

- [1] [PERF03-BP01 Use a purpose-built data store that best supports your data access and storage requirements – Performance Efficiency Pillar] (https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/perf_data_use_purpose_built_data_store.html)
- [3] [Community | Which Data Storage Option Should I Choose?] (<https://community.aws/concepts/which-data-storage-option-do-i-choose>)
- [6] [PERF03-BP01 Use a purpose-built data store that best supports your data access and storage requirements – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2023-10-03/framework/perf_data_use_purpose_built_data_store.html)

解析: Based on the pharmaceutical company's requirements, I recommend deploying an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage. This solution addresses the company's needs in the following ways:

- 1. Scalability: Amazon S3 provides virtually unlimited storage capacity, accommodating the company's exponentially growing data volume.
- 2. Cost-effectiveness: By migrating data to S3, the company can reduce ongoing capital expenses associated with on-premises storage arrays.
- 3. Immediate access to subset data: The file gateway caches frequently accessed data locally, ensuring that researchers can quickly access the subset of data they regularly need with minimal lag.
- 4. Hybrid storage solution: The file gateway acts as a bridge between on-premises systems and Amazon S3, allowing seamless integration with existing workflows and applications.
- 5. Data archiving: Less frequently accessed data can be automatically moved to lower-cost S3 storage tiers, further optimizing costs.

To implement this solution:

1. Set up an Amazon S3 bucket to serve as the target storage.
2. Deploy and configure the AWS

Storage Gateway file gateway appliance on-premises. 3. Migrate the existing data from the on-premises storage arrays to the file gateway. 4. Configure caching policies to ensure frequently accessed data remains readily available. 5. Implement lifecycle policies in S3 to automatically move less frequently accessed data to lower-cost storage tiers. This approach provides a balance between immediate data access for researchers and cost-effective long-term storage for the entire dataset. It also allows for future scalability as the company's data continues to grow. Remember to consult AWS documentation for the most up-to-date information on Storage Gateway and S3 capabilities, pricing, and best practices for your specific use case. Sources [1] [PERF03-BP01 Use a purpose-built data store that best supports your data access and storage requirements – Performance Efficiency Pillar] (https://docs.aws.amazon.com/wellarchitected/latest/performance-efficiency-pillar/perf_data_use_purpose_built_data_store.html) [3] [Community | Which Data Storage Option Should I Choose?] (<https://community.aws/concepts/which-data-storage-option-do-i-choose>) [6] [PERF03-BP01 Use a purpose-built data store that best supports your data access and storage requirements – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2023-10-03/framework/perf_data_use_purpose_built_data_store.html)

665. #Question #768A 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?**

- 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.

答案：A

解析: To enable the company to revert a DynamoDB table to any point within the last 24 hours with the least operational overhead, the solutions architect should configure point-in-time recovery (Option A) for the table. This feature allows for easy restoration of the table to a selected moment in time without the need for manual backup processes or additional storage management.

解析: To enable the company to revert a DynamoDB table to any point within the last 24 hours with the least operational overhead, the solutions architect should configure point-in-time recovery (Option A) for the table. This feature allows for easy restoration of the table to a selected moment in time without the need for manual backup processes or additional storage management.

666. #Question #769A 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 **vary** 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?

- 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.

答案: B

解析: For a cost-effective architecture that can handle variable upload volumes and frequencies, the solutions architect should recommend configuring an object-created event notification within the S3 bucket (Option B). This setup automatically triggers an AWS Lambda function to

process the files as soon as they are uploaded, which is an efficient and scalable approach that aligns with the requirement of processing files to extract metadata within seconds after upload.

解析: For a cost-effective architecture that can handle variable upload volumes and frequencies, the solutions architect should recommend configuring an object-created event notification within the S3 bucket (Option B). This setup automatically triggers an AWS Lambda function to process the files as soon as they are uploaded, which is an efficient and scalable approach that aligns with the requirement of processing files to extract metadata within seconds after upload.

667. #Question #770A 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?

- 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.

答案: C

解析: To optimize costs for the described usage pattern, the most cost-effective solution is to use Compute Savings Plans for the

production instances (Option C), which have constant usage due to customers in different time zones. For nonproduction instances, which are only used during business hours on weekdays, using On-Demand Instances and shutting them down when not in use will minimize costs. This approach ensures that the company pays for reserved capacity for the production environment while only incurring minimal costs for the nonproduction environment that is not used consistently.

解析: To optimize costs for the described usage pattern, the most cost-effective solution is to use Compute Savings Plans for the production instances (Option C), which have constant usage due to customers in different time zones. For nonproduction instances, which are only used during business hours on weekdays, using On-Demand Instances and shutting them down when not in use will minimize costs. This approach ensures that the company pays for reserved capacity for the production environment while only incurring minimal costs for the nonproduction environment that is not used consistently.

668. #Question #771A 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?

- 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.

答案：C

解析：To meet the requirement of capturing changes that occur during the migration from an on-premises Oracle database to Amazon Aurora PostgreSQL, the solutions architect should use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema (Option C). Additionally, AWS Database Migration Service (AWS DMS) should be used to migrate the existing data and to replicate ongoing changes. This combination allows for a seamless migration process and ensures that the Aurora PostgreSQL database is up-to-date with the latest changes from the source Oracle database.

解析：To meet the requirement of capturing changes that occur during the migration from an on-premises Oracle database to Amazon Aurora PostgreSQL, the solutions architect should use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema (Option C). Additionally, AWS Database Migration Service (AWS DMS) should be used to migrate the existing data and to replicate ongoing changes. This combination allows for a seamless migration process and ensures that the Aurora PostgreSQL database is up-to-date with the latest changes from the source Oracle database.

669. #Question #773An 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**?

- 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).

答案：D

解析：To manage sudden traffic increases during a seasonal online sale in a cost-effective manner, the solutions architect should configure an Auto Scaling group (Option D) that scales out as the traffic increases. By using a launch template with a preconfigured Amazon Machine Image (AMI), new instances can be quickly deployed to handle the increased load. This approach ensures that the website can adapt to varying levels of traffic while maintaining cost efficiency by only using the required number of instances at any given time.

解析：To manage sudden traffic increases during a seasonal online sale in a cost-effective manner, the solutions architect should configure an Auto Scaling group (Option D) that scales out as the traffic increases. By using a launch template with a preconfigured Amazon Machine Image (AMI), new instances can be quickly deployed to handle the increased load. This approach ensures that the website can adapt to varying levels of traffic while maintaining cost efficiency by only using the required number of instances at any given time.

670. #Question #774A 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?

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.

答案：B

解析：To meet the requirement of enforcing a compliance policy for security groups and to notify the company of any breach with minimal operational overhead, the solutions architect should enable the restricted-ssh AWS Config managed rule (Option B). This rule automatically checks for security group configurations that allow SSH access from 0.0.0.0/0 and can trigger an Amazon SNS notification if a noncompliant rule is detected. This approach provides an automated and immediate response to policy breaches without the need for custom scripting or additional permissions management.

解析：To meet the requirement of enforcing a compliance policy for security groups and to notify the company of any breach with minimal operational overhead, the solutions architect should enable the restricted-ssh AWS Config managed rule (Option B). This rule automatically checks for security group configurations that allow SSH access from 0.0.0.0/0 and can trigger an Amazon SNS notification if a noncompliant rule is detected. This approach provides an automated and immediate response to policy breaches without the need for custom scripting or additional permissions management.

671. #Question #775Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes. 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**?

- 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.

答案: B

解析: To provide service-to-service communication over HTTPS and a service registry for microservices across different AWS accounts with minimal administrative overhead, the solutions architect should create a VPC Lattice service network (Option B). This service network allows for the definition of HTTPS listeners for each microservice and enables service discovery. It also simplifies the management of network connections between microservices across various VPCs, reducing the complexity and overhead of network management.

解析: To provide service-to-service communication over HTTPS and a service registry for microservices across different AWS accounts with minimal administrative overhead, the solutions architect should create a VPC Lattice service network (Option B). This service network allows for the definition of HTTPS listeners for each microservice and enables service discovery. It also simplifies the management of network connections between microservices across various VPCs, reducing the complexity and overhead of network management.

672. #Question #776A 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?

- 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.

答案: C

解析: Given the requirement for sub-millisecond response times, which indicates the need for low-latency data access, and considering the existing performance issues with the Amazon RDS instance, adding an Amazon ElastiCache for Redis layer (Option C) in front of the database is the recommended solution. Redis can provide in-memory caching, which offers faster access times compared to disk-based storage solutions. This approach will help alleviate the load on the database and improve the game's metadata load times without the need for database migration or changes to the underlying data storage architecture.

解析: Given the requirement for sub-millisecond response times, which indicates the need for low-latency data access, and considering the

existing performance issues with the Amazon RDS instance, adding an Amazon ElastiCache for Redis layer (Option C) in front of the database is the recommended solution. Redis can provide in-memory caching, which offers faster access times compared to disk-based storage solutions. This approach will help alleviate the load on the database and improve the game's metadata load times without the need for database migration or changes to the underlying data storage architecture.

673. #Question #778A 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?

- 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.

答案：B

解析：Considering the global distribution of the offices and the large amount of data to be migrated, using AWS Snowball Edge storage-optimized devices (Option B) is the most cost-effective solution. Snowball Edge can handle the transfer of exabytes of data, making it suitable for the 1 PB of data per office. It is also optimized for high-bandwidth data transfer, which aligns with the available bandwidth at each office. This approach minimizes the time and cost associated with setting up and managing network connections for such a large-scale data migration.

解析：Considering the global distribution of the offices and the large amount of data to be migrated, using AWS Snowball Edge storage-optimized devices (Option B) is the most cost-effective solution. Snowball Edge can handle the transfer of exabytes of data, making it suitable for the 1 PB

of data per office. It is also optimized for high-bandwidth data transfer, which aligns with the available bandwidth at each office. This approach minimizes the time and cost associated with setting up and managing network connections for such a large-scale data migration.

674. #Question #779A 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?

- 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.

答案：B

解析：To meet the company's requirements of allowing read-only access to the Amazon EFS file system containing the reference dataset while preventing modifications or deletions, the best solution is: 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. This solution is the most appropriate because: 1. It uses IAM access control as specified in the requirements. 2. It prevents applications from modifying or deleting the dataset while still allowing read access. 3. It's a centralized approach that can be easily managed and scaled as new EC2 instances or applications are added. Here's how to implement this solution: 1. Create or modify the resource policy

(file system policy) for the EFS file system. 2. In the policy, explicitly allow read access (`elasticfilesystem:ClientMount`) to the IAM roles used by the EC2 instances. 3. Deny the `elasticfilesystem:ClientWrite` action for these same roles. 4. Ensure that the EC2 instances are using the correct IAM roles. This approach follows the principle of least privilege by granting only the necessary permissions for the applications to function while restricting write access. Best practices to consider: 1. Regularly review and audit the resource policy to ensure it remains aligned with security requirements. 2. Use condition keys in the policy to further restrict access based on factors like source IP or encryption requirements. 3. Implement additional security measures such as encryption at rest and in transit for the EFS file system. 4. Monitor access to the file system using AWS CloudTrail and set up alerts for any unauthorized access attempts. Remember to test this configuration in a non-production environment before applying it to your production systems. For the most up-to-date information on EFS security features and best practices, always refer to the official AWS documentation. Sources [1] [Amazon EFS volumes – Amazon Elastic Container Service] (<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>) [3] [Amazon Elastic File System (EFS) | Cloud File Storage | FAQs] (<https://aws.amazon.com/efs/faqs/>) [6] [Using IAM to control file system data access – Amazon Elastic File System] (<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>)

解析: To meet the company's requirements of allowing read-only access to the Amazon EFS file system containing the reference dataset while preventing modifications or deletions, the best solution is: 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. This solution is the most appropriate because: 1. It uses IAM access control as specified in the requirements. 2. It prevents applications from modifying or deleting the dataset while still allowing read access. 3. It's a centralized approach that can be easily managed and scaled as new EC2 instances or applications are added. Here's

how to implement this solution:

1. Create or modify the resource policy (file system policy) for the EFS file system.
2. In the policy, explicitly allow read access (elasticfilesystem:ClientMount) to the IAM roles used by the EC2 instances.
3. Deny the elasticfilesystem:ClientWrite action for these same roles.
4. Ensure that the EC2 instances are using the correct IAM roles. This approach follows the principle of least privilege by granting only the necessary permissions for the applications to function while restricting write access.

Best practices to consider:

1. Regularly review and audit the resource policy to ensure it remains aligned with security requirements.
2. Use condition keys in the policy to further restrict access based on factors like source IP or encryption requirements.
3. Implement additional security measures such as encryption at rest and in transit for the EFS file system.
4. Monitor access to the file system using AWS CloudTrail and set up alerts for any unauthorized access attempts.

Remember to test this configuration in a non-production environment before applying it to your production systems. For the most up-to-date information on EFS security features and best practices, always refer to the official AWS documentation.

Sources

- [1] [Amazon EFS volumes – Amazon Elastic Container Service] (<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>)
- [3] [Amazon Elastic File System (EFS) | Cloud File Storage | FAQs] (<https://aws.amazon.com/efs/faqs/>)
- [6] [Using IAM to control file system data access – Amazon Elastic File System] (<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>)

675. #Question #780A 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?**

- 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.

答案：A

解析：To grant the vendor secure access to the company's AWS account without providing direct access credentials, the most secure approach is to create an IAM role in the company's account (Option A). This role can be given the specific permissions required by the vendor's automated tool. By assuming this role, the vendor's tool can perform necessary actions in the company's AWS account without exposing long-term access credentials. This approach adheres to the principle of least privilege and is considered more secure compared to creating IAM users or modifying permission boundaries.

解析：To grant the vendor secure access to the company's AWS account without providing direct access credentials, the most secure approach is to create an IAM role in the company's account (Option A). This role can be given the specific permissions required by the vendor's automated tool. By assuming this role, the vendor's tool can perform necessary actions in the company's AWS account without exposing long-term access credentials. This approach adheres to the principle of least privilege and is considered more secure compared to creating IAM users or modifying permission boundaries.

676. #Question #781A 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?

- 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.

答案：A

解析：To address the CFO's concerns about cloud spending accountability and to receive notifications when spending reaches 60% of the budget, the solutions architect should use cost allocation tags on AWS resources (Option A). These tags can label resources with the owning department, which is crucial for tracking and allocating costs. Additionally, creating usage budgets in AWS Budgets and setting an alert threshold at 60% of the budget will ensure that the CFO is notified when spending reaches the predetermined threshold. This approach provides direct control and visibility over costs and adheres to the company's budgetary constraints.

解析：To address the CFO's concerns about cloud spending accountability and to receive notifications when spending reaches 60% of the budget, the solutions architect should use cost allocation tags on AWS resources (Option A). These tags can label resources with the owning department, which is crucial for tracking and allocating costs. Additionally, creating usage budgets in AWS Budgets and setting an alert threshold at 60% of the budget will ensure that the CFO is notified when spending reaches the predetermined threshold. This approach provides direct control and visibility over costs and adheres to the company's budgetary

constraints.

677. #Question #782A 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?

- 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.

答案: B

解析: To deploy an internal web application on AWS that is only accessible from the company's office and can download security patches from the internet, the solutions architect should deploy the web application on Amazon EC2 instances in private subnets (Option B). These instances should be placed behind an internal Application Load Balancer (ALB) to ensure that the application is not publicly accessible. NAT

gateways in public subnets will provide the necessary internet access for downloading security patches. An internet gateway attached to the VPC will facilitate the outbound traffic to the internet, and setting the inbound source of the ALB's security group to the company's office network CIDR block will restrict access to the application only to the office network.

解析: To deploy an internal web application on AWS that is only accessible from the company's office and can download security patches from the internet, the solutions architect should deploy the web application on Amazon EC2 instances in private subnets (Option B). These instances should be placed behind an internal Application Load Balancer (ALB) to ensure that the application is not publicly accessible. NAT gateways in public subnets will provide the necessary internet access for downloading security patches. An internet gateway attached to the VPC will facilitate the outbound traffic to the internet, and setting the inbound source of the ALB's security group to the company's office network CIDR block will restrict access to the application only to the office network.

678. #Question #783A 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?

- 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.

答案: D

解析: To migrate the accounting records to an AWS managed service that requires minimal operational support and provides immutable, cryptographically verifiable logs, the most cost-effective solution is to use Amazon Quantum Ledger Database (Amazon QLDB) (Option D). QLDB is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable log of all data changes, which is ideal for applications that require a high degree of data integrity and auditability, such as accounting records.

解析: To migrate the accounting records to an AWS managed service that requires minimal operational support and provides immutable, cryptographically verifiable logs, the most cost-effective solution is to use Amazon Quantum Ledger Database (Amazon QLDB) (Option D). QLDB is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable log of all data changes, which is ideal for applications that require a high degree of data integrity and auditability, such as accounting records.

679. #Question #784A 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?

- 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.

答案: C

解析: To remove the operational overhead of job error handling, retry logic, and state management for the data preparation jobs, the solutions architect should use AWS Glue DataBrew (Option C) to process the data. DataBrew is a visual, user-friendly data preparation tool that enables business analysts to clean and normalize data without writing code. By using an AWS Step Functions state machine, the company can manage the execution of these data preparation jobs in a specific order, ensuring that the jobs run at regular intervals and in parallel as needed, without the need for manual intervention or management of the underlying infrastructure.

解析: To remove the operational overhead of job error handling, retry logic, and state management for the data preparation jobs, the solutions architect should use AWS Glue DataBrew (Option C) to process the data. DataBrew is a visual, user-friendly data preparation tool that enables business analysts to clean and normalize data without writing code. By using an AWS Step Functions state machine, the company can manage the execution of these data preparation jobs in a specific order, ensuring that the jobs run at regular intervals and in parallel as needed, without the need for manual intervention or management of the underlying infrastructure.

680. #Question #785A 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?

- 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.

答案：C

解析：仁者见仁，智者见智，答案C与D都有比较大的争议，各位。 Based on the requirements for the payment processing application, the best solution to ensure that duplicate payments are not processed is: 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. This solution is optimal for several reasons: 1. Idempotency: SQS FIFO (First-In-First-Out) queues provide exactly-once processing, which is crucial for preventing duplicate payments. This addresses the primary requirement of ensuring that the application does not process duplicate payments. 2. Scalability: SQS can handle millions of messages per day, aligning with the application's high transaction volume. 3. Decoupling: Using SQS as a buffer between the payment retrieval and processing steps allows for better fault tolerance and scalability. 4. Ordered Processing: FIFO queues maintain the order of messages, which can be important for certain types of financial transactions. 5. Lambda Integration: AWS Lambda integrates well with SQS, making it easy to trigger functions based on queue events. Best practices and considerations: 1. Message Deduplication: Enable content-based deduplication or use unique deduplication IDs for each payment to prevent duplicate processing. 2. Visibility Timeout: Configure an appropriate visibility timeout for the SQS queue to prevent multiple Lambda functions from processing the same message simultaneously. 3. Dead Letter Queue: Implement a Dead Letter Queue (DLQ) to capture and handle any messages that fail processing after a certain number of attempts. 4. Monitoring: Set up CloudWatch alarms to monitor queue length, processing errors, and Lambda function performance. 5. Error Handling: Implement robust error handling in your Lambda

functions to manage various failure scenarios.

- 6. Encryption: Enable server-side encryption for the SQS queue to protect sensitive payment data.
- 7. VPC Configuration: Ensure that the Lambda functions are properly configured to run in the private subnets across multiple Availability Zones, as mentioned in the requirements.
- 8. Least Privilege: Apply the principle of least privilege when setting up IAM roles for the Lambda functions, granting only the necessary permissions to interact with SQS and other required AWS services.

By implementing this solution with these best practices, you can create a robust, scalable, and secure payment processing application that prevents duplicate payments and meets the specified requirements.

解析：仁者见仁，智者见智，答案C与D都有比较大的争议，各位。 Based on the requirements for the payment processing application, the best solution to ensure that duplicate payments are not processed is: 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. This solution is optimal for several reasons:

- 1. Idempotency: SQS FIFO (First-In-First-Out) queues provide exactly-once processing, which is crucial for preventing duplicate payments. This addresses the primary requirement of ensuring that the application does not process duplicate payments.
- 2. Scalability: SQS can handle millions of messages per day, aligning with the application's high transaction volume.
- 3. Decoupling: Using SQS as a buffer between the payment retrieval and processing steps allows for better fault tolerance and scalability.
- 4. Ordered Processing: FIFO queues maintain the order of messages, which can be important for certain types of financial transactions.
- 5. Lambda Integration: AWS Lambda integrates well with SQS, making it easy to trigger functions based on queue events.

Best practices and considerations:

- 1. Message Deduplication: Enable content-based deduplication or use unique deduplication IDs for each payment to prevent duplicate processing.
- 2. Visibility Timeout: Configure an appropriate visibility timeout for the SQS queue to prevent multiple Lambda functions from processing the same message simultaneously.
- 3. Dead Letter Queue: Implement a Dead Letter

Queue (DLQ) to capture and handle any messages that fail processing after a certain number of attempts. 4. Monitoring: Set up CloudWatch alarms to monitor queue length, processing errors, and Lambda function performance. 5. Error Handling: Implement robust error handling in your Lambda functions to manage various failure scenarios. 6. Encryption: Enable server-side encryption for the SQS queue to protect sensitive payment data. 7. VPC Configuration: Ensure that the Lambda functions are properly configured to run in the private subnets across multiple Availability Zones, as mentioned in the requirements. 8. Least Privilege: Apply the principle of least privilege when setting up IAM roles for the Lambda functions, granting only the necessary permissions to interact with SQS and other required AWS services. By implementing this solution with these best practices, you can create a robust, scalable, and secure payment processing application that prevents duplicate payments and meets the specified requirements.

681. #Question #786A 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?
- 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.

答案：B

解析：To collect usage and configuration data about on-premises servers and workloads for migration planning to AWS, the solutions architect

should use AWS Application Discovery Service (Option B). This service can automatically discover and gather information about the company's on-premises data center, including details about applications, the dependencies between them, and the network configurations. By setting the home AWS Region in AWS Migration Hub and using AWS Application Discovery Service, the company can effectively plan and execute a migration strategy to AWS.

解析: To collect usage and configuration data about on-premises servers and workloads for migration planning to AWS, the solutions architect should use AWS Application Discovery Service (Option B). This service can automatically discover and gather information about the company's on-premises data center, including details about applications, the dependencies between them, and the network configurations. By setting the home AWS Region in AWS Migration Hub and using AWS Application Discovery Service, the company can effectively plan and execute a migration strategy to AWS.

682. #Question #787A 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?

- 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.

答案：A

解析：To meet the company's requirements for auditing all API calls and logins across AWS accounts and ensuring compliance with the AWS Foundational Security Best Practices (FSBP) standard with minimal operational overhead, the solutions architect should deploy an AWS Control Tower environment (Option A). AWS Control Tower provides a centralized governance model and automates the establishment of accounts, including continuous compliance with FSBP. By enabling AWS Security Hub and AWS Control Tower Account Factory within the environment, the company can achieve centralized security and compliance management across all accounts in the organization.

解析：To meet the company's requirements for auditing all API calls and logins across AWS accounts and ensuring compliance with the AWS Foundational Security Best Practices (FSBP) standard with minimal operational overhead, the solutions architect should deploy an AWS Control Tower environment (Option A). AWS Control Tower provides a centralized governance model and automates the establishment of accounts, including continuous compliance with FSBP. By enabling AWS Security Hub and AWS Control Tower Account Factory within the environment, the company can achieve centralized security and compliance management across all accounts in the organization.

683. #Question #788A 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?**

- 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.

答案: C

解析: For a cost-effective solution to analyze log files stored in Apache Parquet format in Amazon S3, the solutions architect should use AWS Glue and Amazon Athena (Option C). AWS Glue can be used to create a crawler that populates the Glue Data Catalog with metadata about the log files. Amazon Athena can then be used to run SQL queries directly against the data in S3, without the need to migrate the data to another database or manage a cluster. This serverless approach minimizes costs by charging only for the queries that are run.

解析: For a cost-effective solution to analyze log files stored in Apache Parquet format in Amazon S3, the solutions architect should use AWS Glue and Amazon Athena (Option C). AWS Glue can be used to create a crawler that populates the Glue Data Catalog with metadata about the log files. Amazon Athena can then be used to run SQL queries directly against the data in S3, without the need to migrate the data to another database or manage a cluster. This serverless approach minimizes costs by charging only for the queries that are run.

684. #Question #789A 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?

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.

答案: D

解析: To prevent AWS CloudFormation from deploying specific resources that do not comply with the company's policy, the solutions architect should use a service control policy (SCP) (Option D). SCPs in AWS Organizations allow the company to define rules that can restrict the actions that can be performed on resources within the organization's accounts. By creating an SCP that blocks actions for EC2 instances and IAM resources when they would result in noncompliance, the company can enforce its policies and prevent the deployment of resources that do not meet the required standards.

解析: To prevent AWS CloudFormation from deploying specific resources that do not comply with the company's policy, the solutions architect should use a service control policy (SCP) (Option D). SCPs in AWS Organizations allow the company to define rules that can restrict the actions that can be performed on resources within the organization's accounts. By creating an SCP that blocks actions for EC2 instances and IAM resources when they would result in noncompliance, the company can enforce its policies and prevent the deployment of resources that do not meet the required standards.

685. #Question #791A 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?

- 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.

答案: D

解析: To ensure that environment variables used by AWS Lambda functions are not visible in plaintext to developers, the solutions architect should create an AWS Key Management Service (AWS KMS) key (Option D). By enabling encryption helpers on the Lambda functions and using the KMS key, the environment variables can be stored and encrypted, providing a secure method for managing sensitive information without exposing it to developers.

解析: To ensure that environment variables used by AWS Lambda functions are not visible in plaintext to developers, the solutions architect should create an AWS Key Management Service (AWS KMS) key (Option D). By enabling encryption helpers on the Lambda functions and using the KMS key, the environment variables can be stored and encrypted, providing a secure method for managing sensitive information without exposing it to developers.

686. #Question #792An 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?

- 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.

答案：A

解析：To offer a web analytics service with RESTful APIs to millions of users while ensuring user authentication, the most operationally efficient solution is to configure an Amazon Cognito user pool (Option A). Amazon Cognito is designed for user authentication and access control in mobile and web applications. By implementing Amazon API Gateway REST APIs with a Cognito authorizer, the analytics company can efficiently manage user authentication at scale without the need for managing custom authentication infrastructure.

解析：To offer a web analytics service with RESTful APIs to millions of users while ensuring user authentication, the most operationally efficient solution is to configure an Amazon Cognito user pool (Option A). Amazon Cognito is designed for user authentication and access control in mobile and web applications. By implementing Amazon API Gateway REST APIs with a Cognito authorizer, the analytics company can efficiently manage user authentication at scale without the need for managing custom authentication infrastructure.

687. #Question #793A 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**?

- 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.

答案：C

解析：To prevent accidental deletion of KMS keys with minimal operational overhead and to notify administrators via email when a deletion attempt occurs, the solutions architect should create an Amazon EventBridge rule (Option C) that triggers upon a KMS DeleteKey operation. This rule can be configured to initiate an AWS Systems Manager Automation runbook that cancels the deletion process. Additionally, the EventBridge rule can be set up to publish a message to an Amazon SNS topic, which then sends an email notification to the administrators. This approach provides a direct and automated response to key deletion attempts with built-in AWS services, minimizing the need for custom development and manual intervention.

解析：To prevent accidental deletion of KMS keys with minimal operational overhead and to notify administrators via email when a deletion attempt occurs, the solutions architect should create an Amazon EventBridge rule (Option C) that triggers upon a KMS DeleteKey operation. This rule can be configured to initiate an AWS Systems Manager Automation runbook that cancels the deletion process. Additionally, the EventBridge rule can be

set up to publish a message to an Amazon SNS topic, which then sends an email notification to the administrators. This approach provides a direct and automated response to key deletion attempts with built-in AWS services, minimizing the need for custom development and manual intervention.

688. #Question #794A 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?

- 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.

答案: B

解析: Considering the company's requirement to generate reports only during the last week of each month and the need for a cost-effective solution, running the program in AWS Lambda (Option B) is the most suitable. Lambda allows the company to run code without provisioning or managing servers, scaling automatically with the size of the workload, and only charging for the compute time consumed. By creating an Amazon EventBridge rule to trigger the Lambda function when reports are needed,

the company can ensure that the reports are generated quickly and at the lowest possible cost during the specified period.

解析: Considering the company's requirement to generate reports only during the last week of each month and the need for a cost-effective solution, running the program in AWS Lambda (Option B) is the most suitable. Lambda allows the company to run code without provisioning or managing servers, scaling automatically with the size of the workload, and only charging for the compute time consumed. By creating an Amazon EventBridge rule to trigger the Lambda function when reports are needed, the company can ensure that the reports are generated quickly and at the lowest possible cost during the specified period.

689. #Question #796A 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?

- 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.

答案: B

解析: To prevent unwanted content in photos uploaded to the company's web application without training an ML model, the solutions architect can create an AWS Lambda function that uses Amazon Rekognition (Option B).

Amazon Rekognition provides pre-trained models for image analysis, which can detect various types of unwanted content. By creating a Lambda function that is triggered by the web application when a new photo is

uploaded, the company can leverage Rekognition's capabilities to scan and analyze the photos, ensuring that only appropriate content is accepted.

解析: To prevent unwanted content in photos uploaded to the company's web application without training an ML model, the solutions architect can create an AWS Lambda function that uses Amazon Rekognition (Option B).

Amazon Rekognition provides pre-trained models for image analysis, which can detect various types of unwanted content. By creating a Lambda function that is triggered by the web application when a new photo is uploaded, the company can leverage Rekognition's capabilities to scan and analyze the photos, ensuring that only appropriate content is accepted.

690. #Question #797A 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?

- 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.

答案: B

解析: To ensure that the company retains access to the root user account in the event of a lost MFA device, the solutions architect should add multiple MFA devices for the root user account (Option B). This approach provides a backup authentication mechanism, allowing the company to maintain access to the AWS account even if the primary MFA device is unavailable. This is a recommended security practice for critical accounts where account access must be protected against device loss or

failure.

解析: To ensure that the company retains access to the root user account in the event of a lost MFA device, the solutions architect should add multiple MFA devices for the root user account (Option B). This approach provides a backup authentication mechanism, allowing the company to maintain access to the AWS account even if the primary MFA device is unavailable. This is a recommended security practice for critical accounts where account access must be protected against device loss or failure.

691. #Question #798A 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?

- 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.

答案：B

解析：To meet the requirement of rapidly adding partners and notifying them through an HTTP endpoint with minimal implementation effort, the solutions architect should create an Amazon Simple Notification Service (Amazon SNS) topic (Option B). By subscribing partners to the SNS topic, the company can easily publish user IDs to the topic, which then gets delivered to all subscribed partners. This approach is highly scalable and requires minimal effort to implement, as it leverages the managed service of Amazon SNS without the need to manage databases, state machines, or data streams.

解析：To meet the requirement of rapidly adding partners and notifying them through an HTTP endpoint with minimal implementation effort, the solutions architect should create an Amazon Simple Notification Service (Amazon SNS) topic (Option B). By subscribing partners to the SNS topic, the company can easily publish user IDs to the topic, which then gets delivered to all subscribed partners. This approach is highly scalable and requires minimal effort to implement, as it leverages the managed service of Amazon SNS without the need to manage databases, state machines, or data streams.

692. Question #799A 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?

- 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 Simple Notification Service (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.

答案：A

解析：Option A is the correct answer because it leverages AWS Lambda and Amazon Comprehend to automatically process and analyze the text files in S3, which is a cost-effective solution that doesn't require in-house machine learning expertise.

解析：Option A is the correct answer because it leverages AWS Lambda and Amazon Comprehend to automatically process and analyze the text files in S3, which is a cost-effective solution that doesn't require in-house machine learning expertise.

693. Question #800A 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?**

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.

答案：B

解析：Option B is the correct answer as it enables direct and secure access to the EFS file system across AWS accounts using VPC peering, without the need for replication or additional Lambda functions, which could increase complexity and cost.

解析：Option B is the correct answer as it enables direct and secure access to the EFS file system across AWS accounts using VPC peering, without the need for replication or additional Lambda functions, which could increase complexity and cost.

694. Question #801A 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?

- 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.**

答案：D

解析：Option D is the correct answer because it allows the company to manage the encryption keys outside of AWS, which is a requirement

specified in the question. By encrypting the data at the data center before it is transferred to S3, the company can maintain full control over the encryption keys.

解析: Option D is the correct answer because it allows the company to manage the encryption keys outside of AWS, which is a requirement specified in the question. By encrypting the data at the data center before it is transferred to S3, the company can maintain full control over the encryption keys.

695. Question #802A 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?

- 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 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.

答案: D

解析: Option D is the correct answer as it provides a serverless architecture that requires minimal operational overhead. Using AWS Lambda for validation and Amazon ECS with Fargate for the backend application allows the company to avoid managing infrastructure while still being able to scale compute and memory resources as needed.

解析: Option D is the correct answer as it provides a serverless architecture that requires minimal operational overhead. Using AWS Lambda for validation and Amazon ECS with Fargate for the backend application allows the company to avoid managing infrastructure while still being able to scale compute and memory resources as needed.

696. Question #803A solutions architect is designing a user authentication solution for a company. The solution must invoke two-factor 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?

- 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).

答案: A

解析: Option A is the correct answer because Amazon Cognito's risk-based adaptive authentication can trigger additional verification steps, such as MFA, based on the risk associated with the login attempt. This feature is designed to scale and is suitable for applications that require secure authentication for a large user base.

解析: Option A is the correct answer because Amazon Cognito's risk-based adaptive authentication can trigger additional verification steps, such as MFA, based on the risk associated with the login attempt. This feature is designed to scale and is suitable for applications that require secure authentication for a large user base.

697. Question #804A 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?

- 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.

答案: C

解析: Option C is the correct answer because it uses AWS Glue, a serverless data integration service, for data transformation and Amazon Redshift Serverless for the data warehouse, which aligns with the requirement to use serverless services. Amazon Redshift ML can be used to create and train ML models using SQL, meeting the need for MPP capabilities and ML model creation.

解析: Option C is the correct answer because it uses AWS Glue, a serverless data integration service, for data transformation and Amazon Redshift Serverless for the data warehouse, which aligns with the requirement to use serverless services. Amazon Redshift ML can be used to create and train ML models using SQL, meeting the need for MPP capabilities and ML model creation.

698. Question #805A 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?

- 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.

答案: C

解析: Option C is the correct answer because AWS Outposts allow you to run AWS services, including Amazon EKS, on-premises in your own data center, which helps maintain data locality and compliance with data storage regulations.

解析: Option C is the correct answer because AWS Outposts allow you to run AWS services, including Amazon EKS, on-premises in your own data center, which helps maintain data locality and compliance with data storage regulations.

699. Question #806A 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?

- 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.

答案：B

解析：Option B is the correct answer as it provides a seamless way to migrate on-premises NFS storage to AWS by using Amazon S3 File Gateway, which allows the use of S3 as a file store with the NFS protocol. This is cost-effective and scalable, and the S3 Lifecycle policy can help manage costs by transitioning data to the appropriate storage class.

解析：Option B is the correct answer as it provides a seamless way to migrate on-premises NFS storage to AWS by using Amazon S3 File Gateway, which allows the use of S3 as a file store with the NFS protocol. This is cost-effective and scalable, and the S3 Lifecycle policy can help manage costs by transitioning data to the appropriate storage class.

700. Question #807A 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?

- 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.

答案: D

解析: Option D is the correct answer because provisioned concurrency can help reduce the latency associated with initializing new Lambda function instances, which is crucial for maintaining service latency. Increasing memory according to AWS Compute Optimizer recommendations can improve the performance of CPU-intensive tasks, potentially reducing the overall compute costs.

解析: Option D is the correct answer because provisioned concurrency can help reduce the latency associated with initializing new Lambda function instances, which is crucial for maintaining service latency. Increasing memory according to AWS Compute Optimizer recommendations can improve the performance of CPU-intensive tasks, potentially reducing the overall compute costs.

701. Question #808A 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?

- 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.

答案：A

解析：Option A is the correct answer because it requires minimal changes to the existing workloads. Amazon ECR can be used to store container images and perform vulnerability scans on them upon push, which integrates well with Amazon ECS.

解析：Option A is the correct answer because it requires minimal changes to the existing workloads. Amazon ECR can be used to store container images and perform vulnerability scans on them upon push, which integrates well with Amazon ECS.

702. Question #809A 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?

- 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.

答案：A

解析：This solution provides the most direct and serverless approach to meet the requirements: EventBridge Rule: EventBridge is used to create a rule that listens to specific events, such as an AWS Batch job transitioning to a "SUCCEEDED" state. This allows the system to react in real time without manual intervention or polling. API Destination: EventBridge supports direct integration with third-party APIs via "API destinations." API destinations provide a seamless way to call an external HTTP API (such as the third-party reporting application) using EventBridge rules. Authentication: API destinations in EventBridge allow specifying authentication methods like username and password. This aligns with the requirement of using HTTP API authentication based on a username and password. Serverless Design: This approach does not require any additional infrastructure, such as Lambda functions or API Gateway, making it completely serverless and efficient. Other Options: B: Using EventBridge with an AWS Lambda function adds unnecessary complexity, as API destinations can directly invoke the third-party API without the need for Lambda. C: Using AWS Batch to publish events to an API Gateway REST API introduces additional infrastructure and operational overhead. EventBridge already supports this use case natively with API destinations. D: This approach is similar to option C but adds Lambda for invoking the third-party API, further increasing complexity unnecessarily. Why A is the Best Choice: Option A uses the native capabilities of Amazon EventBridge to directly invoke the third-party API. It simplifies the architecture, minimizes infrastructure overhead, and adheres to the requirements for serverless operation and HTTP authentication.

解析：This solution provides the most direct and serverless approach to meet the requirements: EventBridge Rule: EventBridge is used to create a rule that listens to specific events, such as an AWS Batch job

transitioning to a "SUCCEEDED" state. This allows the system to react in real time without manual intervention or polling.

API Destination: EventBridge supports direct integration with third-party APIs via "API destinations." API destinations provide a seamless way to call an external HTTP API (such as the third-party reporting application) using EventBridge rules.

Authentication: API destinations in EventBridge allow specifying authentication methods like username and password. This aligns with the requirement of using HTTP API authentication based on a username and password.

Serverless Design: This approach does not require any additional infrastructure, such as Lambda functions or API Gateway, making it completely serverless and efficient.

Other Options:

- B:** Using EventBridge with an AWS Lambda function adds unnecessary complexity, as API destinations can directly invoke the third-party API without the need for Lambda.
- C:** Using AWS Batch to publish events to an API Gateway REST API introduces additional infrastructure and operational overhead.
- D:** This approach is similar to option C but adds Lambda for invoking the third-party API, further increasing complexity unnecessarily.

Why A is the Best Choice: Option A uses the native capabilities of Amazon EventBridge to directly invoke the third-party API. It simplifies the architecture, minimizes infrastructure overhead, and adheres to the requirements for serverless operation and HTTP authentication.

703. Question #810A 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?

- 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.

答案: C

解析: Option C is the correct answer because it enables private and secure access to the RDS database using AWS PrivateLink, which does not require an internet gateway, Direct Connect, or VPN connection. By placing an NLB in front of the RDS instance and setting up a VPC endpoint service, the company can access the database without exposing it to the public internet.

解析: Option C is the correct answer because it enables private and secure access to the RDS database using AWS PrivateLink, which does not require an internet gateway, Direct Connect, or VPN connection. By placing an NLB in front of the RDS instance and setting up a VPC endpoint service, the company can access the database without exposing it to the public internet.

704. Question #811A 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?

- 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 VPC. Create 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.

答案：B

解析：To set up Amazon Managed Grafana as a visualization tool for an Amazon RDS database while ensuring a secure solution that doesn't expose data over the internet, the recommended approach is as follows: Overview: We'll create an Amazon Managed Grafana workspace in a VPC and configure it to securely connect to an Amazon RDS database using a private endpoint. This setup ensures that data visualization can be performed without exposing sensitive information to the public internet. Here's a step-by-step guide to accomplish this task:

1. **Set up Amazon Managed Grafana Workspace**
 - Navigate to the Amazon Managed Grafana console
 - Create a new workspace
 - Choose to deploy the workspace in a VPC
 - Select an existing VPC or create a new one for this purpose
2. **Configure Amazon RDS Database**
 - Ensure your RDS database is deployed in the same VPC as the Managed Grafana workspace
 - If not already done, move the RDS instance into the VPC
 - Configure the database to use a private endpoint
 - Update security groups to allow traffic from the Managed Grafana workspace
3. **Set up VPC Connectivity**
 - Ensure proper routing is configured between the Managed Grafana workspace and the RDS database subnets
 - Configure Network ACLs and security groups to allow necessary traffic between Managed Grafana and RDS
4. **Configure Data Source in Managed Grafana**
 - Access your Managed Grafana workspace
 - Add a new data source, selecting the appropriate database type (e.g., MySQL, PostgreSQL)
 - Use the private endpoint of your RDS database as the connection string
 - Configure authentication using secure credentials (consider using AWS Secrets Manager for credential management)
5. **Test and Verify Connection**
 - Use Grafana's built-in

connection test feature to ensure successful connectivity to the RDS database – Create a sample dashboard to verify data retrieval and visualization 6. ****Implement Additional Security Measures**** – Enable encryption at rest for both Managed Grafana and RDS – Implement proper IAM roles and policies for access control – Consider using AWS IAM Identity Center for user authentication and authorization in Managed Grafana Recap: By following these steps, you've created a secure visualization solution using Amazon Managed Grafana and Amazon RDS. The Managed Grafana workspace is deployed within a VPC and connects to the RDS database using a private endpoint, ensuring that data remains within the AWS network and is not exposed to the public internet. This setup provides a robust and secure foundation for data visualization while maintaining the confidentiality of your database information. Sources [1] [What is Amazon Managed Grafana? – Amazon Managed Grafana] (<https://docs.aws.amazon.com/grafana/latest/userguide/what-is-Amazon-Managed-Service-Grafana.html>) [3] [Security in Amazon RDS – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html>) [6] [Amazon Managed Grafana for dashboarding and visualization – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/amg-dashboarding-visualization.html>)

解析: To set up Amazon Managed Grafana as a visualization tool for an Amazon RDS database while ensuring a secure solution that doesn't expose data over the internet, the recommended approach is as follows: Overview: We'll create an Amazon Managed Grafana workspace in a VPC and configure it to securely connect to an Amazon RDS database using a private endpoint. This setup ensures that data visualization can be performed without exposing sensitive information to the public internet. Here's a step-by-step guide to accomplish this task:

1. ****Set up Amazon Managed Grafana Workspace**** – Navigate to the Amazon Managed Grafana console – Create a new workspace – Choose to deploy the workspace in a VPC – Select an existing VPC or create a new one for this purpose – Configure appropriate subnets and security groups
2. ****Configure Amazon RDS Database**** – Ensure your RDS database is deployed in the same VPC

as the Managed Grafana workspace

- If not already done, move the RDS instance into the VPC
- Configure the database to use a private endpoint
- Update security groups to allow traffic from the Managed Grafana workspace

3. ****Set up VPC Connectivity****

- Ensure proper routing is configured between the Managed Grafana workspace and the RDS database subnets
- Configure Network ACLs and security groups to allow necessary traffic between Managed Grafana and RDS

4. ****Configure Data Source in Managed Grafana****

- Access your Managed Grafana workspace
- Add a new data source, selecting the appropriate database type (e.g., MySQL, PostgreSQL)
- Use the private endpoint of your RDS database as the connection string
- Configure authentication using secure credentials (consider using AWS Secrets Manager for credential management)

5. ****Test and Verify Connection****

- Use Grafana's built-in connection test feature to ensure successful connectivity to the RDS database
- Create a sample dashboard to verify data retrieval and visualization

6. ****Implement Additional Security Measures****

- Enable encryption at rest for both Managed Grafana and RDS
- Implement proper IAM roles and policies for access control
- Consider using AWS IAM Identity Center for user authentication and authorization in Managed Grafana

Recap: By following these steps, you've created a secure visualization solution using Amazon Managed Grafana and Amazon RDS. The Managed Grafana workspace is deployed within a VPC and connects to the RDS database using a private endpoint, ensuring that data remains within the AWS network and is not exposed to the public internet. This setup provides a robust and secure foundation for data visualization while maintaining the confidentiality of your database information.

Sources [1] [What is Amazon Managed Grafana? – Amazon Managed Grafana] (<https://docs.aws.amazon.com/grafana/latest/userguide/what-is-Amazon-Managed-Service-Grafana.html>) [3] [Security in Amazon RDS – Amazon Relational Database Service] (<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html>) [6] [Amazon Managed Grafana for dashboarding and visualization – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/amg-dashboarding-visualization.html>)

705. Question #812A 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?

- 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.

答案：C

解析：Option C is the correct answer because AWS Glue DataBrew is a visual, user-friendly tool that enables data preparation without writing code. It supports data transformation, data lineage, and data profiling. DataBrew recipes can be shared with other employees, making it easy to collaborate on data transformation steps.

解析：Option C is the correct answer because AWS Glue DataBrew is a visual, user-friendly tool that enables data preparation without writing code. It supports data transformation, data lineage, and data profiling. DataBrew recipes can be shared with other employees, making it easy to collaborate on data transformation steps.

706. Question #813A 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?

- 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.

答案: A

解析: Option A is the correct answer because it allows for routing to a specific EC2 instance via the ALB without exposing the instance's public IP address. The use of an ALB listener rule ensures that traffic for the development website is directed to the correct target group, and this routing can be updated without changing the A Record if the development instance is replaced.

解析: Option A is the correct answer because it allows for routing to a specific EC2 instance via the ALB without exposing the instance's public IP address. The use of an ALB listener rule ensures that traffic for the

development website is directed to the correct target group, and this routing can be updated without changing the A Record if the development instance is replaced.

707. Question #814A 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?

- 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.

答案：B

解析：Option B is the correct answer because it provides a migration path to AWS with minimal changes to the existing application architecture.

Since the application already uses AMQP, Amazon MQ is a natural fit as it supports AMQP out of the box. Migrating to Amazon EKS allows the company to take advantage of a managed Kubernetes service, which reduces operational overhead compared to managing a Kubernetes cluster on-premises or using EC2 instances directly.

解析：Option B is the correct answer because it provides a migration path to AWS with minimal changes to the existing application architecture.

Since the application already uses AMQP, Amazon MQ is a natural fit as it supports AMQP out of the box. Migrating to Amazon EKS allows the company to take advantage of a managed Kubernetes service, which reduces operational overhead compared to managing a Kubernetes cluster

on-premises or using EC2 instances directly.

708. Question #815 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?

- 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.**

答案: D

解析: Option D is the correct answer because AWS Global Accelerator is designed to improve the performance of applications with a global presence by routing user traffic to the nearest or **最优的** endpoint. By using AWS Global Accelerator, the gaming company can reduce the load time experienced by customers around the world, as it directs traffic to the most appropriate NLB based on factors like location and health.

解析: Option D is the correct answer because AWS Global Accelerator is designed to improve the performance of applications with a global presence by routing user traffic to the nearest or **最优的** endpoint. By using AWS Global Accelerator, the gaming company can reduce the load time experienced by customers around the world, as it directs traffic to the most appropriate NLB based on factors like location and health.

709. Question #816 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?

- 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.

答案: B

解析: Option B is the correct answer because AWS Transfer Family provides a managed service for SFTP that can integrate with Amazon S3, allowing vendors to continue using their SFTP clients to transfer files directly to S3, which minimizes the operational overhead for the company.

解析: Option B is the correct answer because AWS Transfer Family provides a managed service for SFTP that can integrate with Amazon S3, allowing vendors to continue using their SFTP clients to transfer files directly to S3, which minimizes the operational overhead for the company.

710. Question #817A 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?

- 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.

答案: C

解析: Option C is the correct answer because Amazon Textract can be used to extract text and data from PDFs, and the insights can then be passed directly to Amazon Comprehend for sentiment analysis. This workflow requires minimal additional infrastructure and is integrated, which reduces operational overhead compared to the other options.

解析: Option C is the correct answer because Amazon Textract can be used to extract text and data from PDFs, and the insights can then be passed directly to Amazon Comprehend for sentiment analysis. This workflow requires minimal additional infrastructure and is integrated, which reduces operational overhead compared to the other options.

711. Question #818A 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?

- 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 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.

答案：A

解析：Option A is the correct answer because Amazon Kinesis Data Firehose is a fully managed service that can directly capture and automatically load streaming data into an S3 bucket, which is ideal for real-time data ingestion at scale.

解析：Option A is the correct answer because Amazon Kinesis Data Firehose is a fully managed service that can directly capture and automatically load streaming data into an S3 bucket, which is ideal for real-time data ingestion at scale.

712. Question #819A 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?

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.

答案: B

解析: Option B is the correct answer because it provides a scalable solution for storing large data items that exceed DynamoDB's size limits. By storing the large data in S3 and maintaining a reference in DynamoDB, the company can leverage the high durability and availability of S3 while still using DynamoDB for metadata and smaller items.

解析: Option B is the correct answer because it provides a scalable solution for storing large data items that exceed DynamoDB's size limits. By storing the large data in S3 and maintaining a reference in DynamoDB, the company can leverage the high durability and availability of S3 while still using DynamoDB for metadata and smaller items.

713. Question #820A 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?

- 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.

答案: C

解析: Option C is the correct answer because it allows the company to migrate cron jobs to a serverless environment with minimal changes. AWS Fargate can run containerized applications without the need to manage the underlying infrastructure, and EventBridge can handle the scheduling based on a recurring schedule.

解析: Option C is the correct answer because it allows the company to migrate cron jobs to a serverless environment with minimal changes. AWS Fargate can run containerized applications without the need to manage the underlying infrastructure, and EventBridge can handle the scheduling based on a recurring schedule.

714. Question #821A 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?

- 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.

答案: C

解析: Option C is the correct answer because AWS PrivateLink provides a private connection between the VPC and Salesforce, and Amazon AppFlow can be used to transfer data without the need for extensive development effort. This solution is secure and does not require the data to travel over the public internet.

解析: Option C is the correct answer because AWS PrivateLink provides a private connection between the VPC and Salesforce, and Amazon AppFlow can be used to transfer data without the need for extensive development effort. This solution is secure and does not require the data to travel

over the public internet.

715. Question #822A 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?

- 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.

答案：A

解析：Option A is the correct answer because Amazon S3's Intelligent-Tiering automatically moves files to the most cost-effective storage access tier without operational overhead or additional action. This can significantly reduce storage costs while still providing access to the data as needed.

解析：Option A is the correct answer because Amazon S3's Intelligent-Tiering automatically moves files to the most cost-effective storage access tier without operational overhead or additional action. This can significantly reduce storage costs while still providing access to the data as needed.

716. Question #823A 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?

- 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.

答案: C

解析: Option C is the correct answer because an Application Load Balancer (ALB) supports routing based on query parameters, which is a requirement specified in the question. Additionally, ALBs can be configured to use HTTPS, which requires an SSL/TLS certificate to encrypt traffic, and AWS Certificate Manager can provide these certificates.

解析: Option C is the correct answer because an Application Load Balancer (ALB) supports routing based on query parameters, which is a requirement specified in the question. Additionally, ALBs can be configured to use HTTPS, which requires an SSL/TLS certificate to encrypt traffic, and AWS Certificate Manager can provide these certificates.

717. Question #824A 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?

- 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.

答案: C

解析: Option C is the correct answer because Amazon Aurora Serverless is a MySQL-compatible relational database that automatically starts and stops compute resources based on your schema setup, which provides scalability and high availability without the need for manual intervention.

解析: Option C is the correct answer because Amazon Aurora Serverless is a MySQL-compatible relational database that automatically starts and stops compute resources based on your schema setup, which provides scalability and high availability without the need for manual intervention.

718. Question #825A 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?**

- 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.

答案：B

解析：Option B is the correct answer because it allows the company to use AWS KMS for encryption and key management, including automatic key rotation, which meets the requirement for automatic key rotation every year with minimal operational overhead.

解析：Option B is the correct answer because it allows the company to use AWS KMS for encryption and key management, including automatic key rotation, which meets the requirement for automatic key rotation every year with minimal operational overhead.

719. Question #826A company is migrating applications from an on-premises Microsoft Active Directory that the company manages to 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?

- A. Create an Enterprise Edition Active Directory in AWS Directory Service for Microsoft Active Directory. 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.

答案: B

解析: Option B is the correct answer because it enables the company to use its existing on-premises Active Directory as the source of truth for user and group management while providing a single sign-on solution across all AWS accounts through AWS IAM Identity Center and a two-way forest trust relationship.

解析: Option B is the correct answer because it enables the company to use its existing on-premises Active Directory as the source of truth for user and group management while providing a single sign-on solution across all AWS accounts through AWS IAM Identity Center and a two-way forest trust relationship.

720. Question #827A 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?

- 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.

答案: D

解析: To optimize the storage performance of an Amazon Aurora PostgreSQL Serverless v2 cluster for an application that will receive large amounts of traffic, while maintaining cost-effectiveness, the most suitable solution is: D. Configure the cluster to use the Aurora I/O-Optimized storage configuration. Here's why this is the most cost-effective

solution:

1. **Performance Optimization:** Aurora I/O-Optimized is designed to provide better performance for I/O-intensive workloads, which aligns well with the application's expected large amounts of traffic.
2. **Cost-Effectiveness:** While I/O-Optimized may have a slightly higher base cost than Standard storage, it can be more cost-effective for high-traffic applications. The improved I/O performance can reduce the need for over-provisioning compute resources, potentially leading to overall cost savings.
3. **Scalability:** Aurora I/O-Optimized works well with Serverless v2, allowing the database to scale compute resources independently of storage, which is ideal for applications with variable workloads.
4. **Automatic Management:** With Serverless v2, you don't need to manually provision IOPS or choose specific storage types like General Purpose or Provisioned IOPS. The I/O-Optimized configuration automatically manages storage performance based on workload.
5. **Compatibility:** Aurora I/O-Optimized is available for PostgreSQL versions supported by Aurora Serverless v2, ensuring compatibility with your chosen database engine.

Best practices when implementing this solution:

1. Monitor performance metrics closely, especially during peak traffic periods, to ensure the I/O-Optimized configuration meets your needs.
2. Use Amazon CloudWatch to track key metrics like ACUUtilization, CPUUtilization, and FreeableMemory to optimize your Serverless v2 configuration.
3. Consider setting appropriate minimum and maximum ACU values for your Serverless v2 cluster to balance performance and cost.
4. Implement proper security measures, such as encryption at rest and in transit, and use AWS Identity and Access Management (IAM) for access control.
5. Regularly review and optimize your database queries and schema to ensure efficient use of the I/O-Optimized storage. Remember to consult the AWS documentation for the most up-to-date information on Aurora PostgreSQL Serverless v2 and I/O-Optimized storage configuration, as features and recommendations may evolve over time.

Sources [1] [Supported Regions and Aurora DB engines for cluster storage configurations – Amazon Aurora] (https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.storage-type.html) [3] [Improved memory management in Aurora PostgreSQL – Amazon

Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.BestPractices.memory.management.html>) [6] [Performance and scaling for Amazon Aurora PostgreSQL – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Managing.html>)

解析: To optimize the storage performance of an Amazon Aurora PostgreSQL Serverless v2 cluster for an application that will receive large amounts of traffic, while maintaining cost-effectiveness, the most suitable solution is: D. Configure the cluster to use the Aurora I/O-Optimized storage configuration. Here's why this is the most cost-effective solution:

1. **Performance Optimization:** Aurora I/O-Optimized is designed to provide better performance for I/O-intensive workloads, which aligns well with the application's expected large amounts of traffic.
2. **Cost-Effectiveness:** While I/O-Optimized may have a slightly higher base cost than Standard storage, it can be more cost-effective for high-traffic applications. The improved I/O performance can reduce the need for over-provisioning compute resources, potentially leading to overall cost savings.
3. **Scalability:** Aurora I/O-Optimized works well with Serverless v2, allowing the database to scale compute resources independently of storage, which is ideal for applications with variable workloads.
4. **Automatic Management:** With Serverless v2, you don't need to manually provision IOPS or choose specific storage types like General Purpose or Provisioned IOPS. The I/O-Optimized configuration automatically manages storage performance based on workload.
5. **Compatibility:** Aurora I/O-Optimized is available for PostgreSQL versions supported by Aurora Serverless v2, ensuring compatibility with your chosen database engine.

Best practices when implementing this solution:

1. Monitor performance metrics closely, especially during peak traffic periods, to ensure the I/O-Optimized configuration meets your needs.
2. Use Amazon CloudWatch to track key metrics like ACUUtilization, CPUUtilization, and FreeableMemory to optimize your Serverless v2 configuration.
3. Consider setting appropriate minimum and maximum ACU values for your Serverless v2 cluster to balance performance and cost.
4. Implement proper security measures, such as encryption at rest and in

transit, and use AWS Identity and Access Management (IAM) for access control. 5. Regularly review and optimize your database queries and schema to ensure efficient use of the I/O-Optimized storage. Remember to consult the AWS documentation for the most up-to-date information on Aurora PostgreSQL Serverless v2 and I/O-Optimized storage configuration, as features and recommendations may evolve over time. Sources [1] [Supported Regions and Aurora DB engines for cluster storage configurations – Amazon Aurora] (https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.storage-type.html) [3] [Improved memory management in Aurora PostgreSQL – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.BestPractices.memory.management.html>) [6] [Performance and scaling for Amazon Aurora PostgreSQL – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Managing.html>)

721. Question #828A 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?

- 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.

答案：D

解析：Option D is the correct answer because AWS Security Hub provides a comprehensive view of the security state of the resources across all AWS accounts in an organization. It can also be used to enable security standards that comply with industry standards like NIST and PCI DSS, which is necessary for third-party auditors to verify the implementation of security controls.

解析：Option D is the correct answer because AWS Security Hub provides a comprehensive view of the security state of the resources across all AWS accounts in an organization. It can also be used to enable security standards that comply with industry standards like NIST and PCI DSS, which is necessary for third-party auditors to verify the implementation of security controls.

722. Question #829A 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?

- 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.

答案：A

解析：Option A is the correct answer because S3 Intelligent-Tiering automatically moves objects between access tiers based on access patterns, which can reduce storage costs while maintaining immediate availability for frequently accessed objects without requiring manual intervention or operational changes.

解析：Option A is the correct answer because S3 Intelligent-Tiering automatically moves objects between access tiers based on access patterns, which can reduce storage costs while maintaining immediate availability for frequently accessed objects without requiring manual intervention or operational changes.

723. Question #830A 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?

- 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.

答案：B

解析：Option B is the correct answer because Amazon Neptune is a fully managed graph database service that can efficiently handle highly connected data and complex traversal operations, such as finding mutual

connections up to multiple levels.

解析: Option B is the correct answer because Amazon Neptune is a fully managed graph database service that can efficiently handle highly connected data and complex traversal operations, such as finding mutual connections up to multiple levels.

724. Question #831A 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?

- 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.

答案: D

解析: old(A) --> new(D) old: Option A is the correct answer because a client VPN can be set up quickly and is suitable for lower bandwidth requirements. It is also a more cost-effective solution compared to AWS Direct Connect or a Site-to-Site VPN, which may be overprovisioned for small amounts of traffic.

解析: old(A) --> new(D) old: Option A is the correct answer because a client VPN can be set up quickly and is suitable for lower bandwidth requirements. It is also a more cost-effective solution compared to AWS Direct Connect or a Site-to-Site VPN, which may be overprovisioned for small amounts of traffic.

725. Question #832A 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?

- 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.

答案：C

解析：Option C is the correct answer because AWS Transfer Family can be integrated with the company's existing on-premises Active Directory using AD Connector. This allows the company to maintain the current authentication mechanism with minimal operational overhead and simplifies the migration process.

解析：Option C is the correct answer because AWS Transfer Family can be integrated with the company's existing on-premises Active Directory using AD Connector. This allows the company to maintain the current authentication mechanism with minimal operational overhead and simplifies the migration process.

726. Question #833A 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?

- 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.

答案: C

解析: Option C is the correct answer because Amazon EventBridge can decouple the components of the order processing system by using event rules that trigger specific Lambda functions based on the event pattern. Input transformers can be used to ensure that each Lambda function receives only the relevant portion of the order event data, which aligns with the requirement for loose coupling and future adaptability.

解析: Option C is the correct answer because Amazon EventBridge can decouple the components of the order processing system by using event rules that trigger specific Lambda functions based on the event pattern. Input transformers can be used to ensure that each Lambda function receives only the relevant portion of the order event data, which aligns with the requirement for loose coupling and future adaptability.

727. Question #834A 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?

- 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.

答案: C

解析: Option C is the correct answer because Amazon Aurora MySQL's Multi-AZ deployment with read replicas can improve performance by allowing read traffic to be distributed across the replicas. This can help to offload some of the database load during peak times, which can alleviate the performance issues experienced when generating real-time reports.

解析: Option C is the correct answer because Amazon Aurora MySQL's Multi-AZ deployment with read replicas can improve performance by allowing read traffic to be distributed across the replicas. This can help to offload some of the database load during peak times, which can alleviate the performance issues experienced when generating real-time reports.

728. Question #835A 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**?

- 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.

答案: C

解析: Option C is the correct answer because an Amazon S3 interface endpoint allows traffic to be routed directly from the on-premises network to the S3 service within the AWS network, without the need for a public VIF or a NAT gateway. This can reduce costs associated with data transfer and provide a secure connection to S3.

解析: Option C is the correct answer because an Amazon S3 interface endpoint allows traffic to be routed directly from the on-premises network to the S3 service within the AWS network, without the need for a public VIF or a NAT gateway. This can reduce costs associated with data transfer and provide a secure connection to S3.

729. Question #836A 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 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?

- 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

答案: B

解析: Option B is the correct answer because Amazon Route 53's multivalue answer routing policy can return multiple IP addresses for healthy resources, allowing traffic to be distributed across multiple Regions. This can help to ensure high availability and fault tolerance for the website.

解析: Option B is the correct answer because Amazon Route 53's multivalue answer routing policy can return multiple IP addresses for healthy resources, allowing traffic to be distributed across multiple Regions. This can help to ensure high availability and fault tolerance for the website.

730. Question #837A 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?

- 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.

答案: C

解析: Option C is the correct answer because Amazon EFS provides a scalable, elastic file system that can be mounted on multiple EC2

instances, making it suitable for applications that require access to large files across various instances and Availability Zones.

解析: Option C is the correct answer because Amazon EFS provides a scalable, elastic file system that can be mounted on multiple EC2 instances, making it suitable for applications that require access to large files across various instances and Availability Zones.

731. Question #838A 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?**

- 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.

答案: D

解析: Option D is the correct answer because it provides a straightforward method to encrypt both EBS volumes and RDS database volumes using AWS KMS, which requires minimal changes to the existing infrastructure and helps meet compliance requirements for data at rest encryption.

解析: Option D is the correct answer because it provides a straightforward method to encrypt both EBS volumes and RDS database volumes using AWS KMS, which requires minimal changes to the existing infrastructure and helps meet compliance requirements for data at rest encryption.

732. Question #839A 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?

- 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 VPC. Update 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.

答案：C

解析：Option C is the correct answer because a VPC endpoint for Amazon S3 allows traffic to flow directly to and from Amazon S3 through the AWS network without using the internet, which reduces the load on the NAT instance and eliminates the need for a public route.

解析：Option C is the correct answer because a VPC endpoint for Amazon S3 allows traffic to flow directly to and from Amazon S3 through the AWS network without using the internet, which reduces the load on the NAT instance and eliminates the need for a public route.

733. Question #840A 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?

- A. Amazon CloudFront

- B. AWS Global Accelerator
- C. AWS Client VPN
- D. Amazon EC2 instances and AWS Elastic IP addresses

答案：B

解析：Option B is the correct answer because AWS Global Accelerator can improve the performance of TCP traffic by directing it through the optimal AWS region, which can enhance the quality of live streams sent by reporters. It is designed to improve the user experience for applications with a global footprint, which is suitable for a news company with a worldwide presence.

解析：Option B is the correct answer because AWS Global Accelerator can improve the performance of TCP traffic by directing it through the optimal AWS region, which can enhance the quality of live streams sent by reporters. It is designed to improve the user experience for applications with a global footprint, which is suitable for a news company with a worldwide presence.

734. Question #6A 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?

- 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.

答案：B

解析：The use of AWS Snowball Edge allows for the physical transfer of data, bypassing the need for network bandwidth for the migration. This is particularly useful for large data sets where network transfer would be costly and time-consuming. Once the Snowball Edge device is returned to AWS, the data is uploaded to S3, fulfilling the requirement of migrating the data as soon as possible with minimal use of network bandwidth.

解析：The use of AWS Snowball Edge allows for the physical transfer of data, bypassing the need for network bandwidth for the migration. This is particularly useful for large data sets where network transfer would be costly and time-consuming. Once the Snowball Edge device is returned to AWS, the data is uploaded to S3, fulfilling the requirement of migrating the data as soon as possible with minimal use of network bandwidth.

735. Question #841A 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.2. 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?

- 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.

答案：B

解析：Based on the company's requirements for long-term snapshot retention and cost-effectiveness, the most suitable solution is: 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. Here's why this solution is the most cost-effective and meets the requirements:

- 1. Compliance: EBS Snapshots Archive is designed for long-term retention, making it suitable for the 7-year retention requirement imposed by the new regulations.
- 2. Cost-effectiveness:
 - Daily snapshots remain in the standard tier for 1 month, which is appropriate for short-term operational recovery.
 - Monthly snapshots are moved to the archive tier, which is significantly cheaper for long-term storage compared to the standard tier.
- 3. Minimal administrative effort:
 - The existing daily snapshot policy can remain unchanged.
 - A new policy can be set up to automatically move monthly snapshots to the archive tier, reducing manual intervention.
- 4. Data availability: While archived snapshots take longer to restore (up to 72 hours), this is acceptable for long-term compliance data that is rarely accessed.
- 5. Seamless integration: Using EBS Snapshots Archive keeps all snapshot management within the EBS ecosystem, simplifying operations and reducing complexity compared to moving data to a different service like S3 Glacier Deep Archive.

Implementation considerations:

- 1. Set up a lifecycle policy to automatically move monthly snapshots to the archive tier.
- 2. Ensure the archive retention period is set to 7 years to meet the regulatory requirements.
- 3. Monitor costs and adjust policies if needed, as archiving very frequent snapshots can sometimes be more

expensive than keeping them in the standard tier. 4. Implement appropriate IAM policies to control access to both standard and archived snapshots. 5. Regularly test the restore process for archived snapshots to ensure data can be retrieved when needed. Remember to consult the AWS documentation for the most up-to-date information on EBS Snapshots Archive, including pricing details and any service limitations. Sources [1] [Guidelines and best practices for archiving Amazon EBS snapshots – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/archiving-guidelines.html>) [3] [Save on storage costs using Amazon S3] (<https://aws.amazon.com/s3/cost-optimization/>) [6] [RetentionArchiveTier – Amazon Data Lifecycle Manager] (https://docs.aws.amazon.com/dlm/latest/APIReference/API_RetentionArchiveTier.html)

解析: Based on the company's requirements for long-term snapshot retention and cost-effectiveness, the most suitable solution is: 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. Here's why this solution is the most cost-effective and meets the requirements: 1. Compliance: EBS Snapshots Archive is designed for long-term retention, making it suitable for the 7-year retention requirement imposed by the new regulations. 2. Cost-effectiveness: – Daily snapshots remain in the standard tier for 1 month, which is appropriate for short-term operational recovery. – Monthly snapshots are moved to the archive tier, which is significantly cheaper for long-term storage compared to the standard tier. 3. Minimal administrative effort: – The existing daily snapshot policy can remain unchanged. – A new policy can be set up to automatically move monthly snapshots to the archive tier, reducing manual intervention. 4. Data availability: While archived snapshots take longer to restore (up to 72 hours), this is acceptable for long-term compliance data that is rarely accessed. 5. Seamless integration: Using EBS Snapshots Archive keeps all snapshot management within the EBS ecosystem, simplifying operations and reducing complexity compared to moving data to a different service like S3 Glacier Deep Archive. Implementation considerations: 1. Set up a lifecycle policy to automatically move monthly snapshots to the

archive tier. 2. Ensure the archive retention period is set to 7 years to meet the regulatory requirements. 3. Monitor costs and adjust policies if needed, as archiving very frequent snapshots can sometimes be more expensive than keeping them in the standard tier. 4. Implement appropriate IAM policies to control access to both standard and archived snapshots. 5. Regularly test the restore process for archived snapshots to ensure data can be retrieved when needed. Remember to consult the AWS documentation for the most up-to-date information on EBS Snapshots Archive, including pricing details and any service limitations. Sources [1] [Guidelines and best practices for archiving Amazon EBS snapshots – Amazon EBS] (<https://docs.aws.amazon.com/ebs/latest/userguide/archiving-guidelines.html>) [3] [Save on storage costs using Amazon S3] (<https://aws.amazon.com/s3/cost-optimization/>) [6] [RetentionArchiveTier – Amazon Data Lifecycle Manager] (https://docs.aws.amazon.com/dlm/latest/APIReference/API_RetentionArchiveTier.html)

736. Question #842A 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?

- 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.

答案：A

解析：The most cost-effective solution for replicating data from an Amazon EFS to another AWS Region is to use the native EFS Replication feature. This service is designed to handle the replication of EFS data

across regions with minimal configuration and operational overhead.

解析: The most cost-effective solution for replicating data from an Amazon EFS to another AWS Region is to use the native EFS Replication feature. This service is designed to handle the replication of EFS data across regions with minimal configuration and operational overhead.

737. Question #843An 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**?

- 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.

答案: C

解析: The solution that meets the requirements of high availability and scalability with the least administrative overhead is to migrate the web application to Amazon EC2 instances within an Auto Scaling group, ensuring that it can handle increased load during peak times. For the database, using Amazon RDS with Multi-AZ deployment provides a managed,

highly available database solution that requires minimal administrative effort.

解析: The solution that meets the requirements of high availability and scalability with the least administrative overhead is to migrate the web application to Amazon EC2 instances within an Auto Scaling group, ensuring that it can handle increased load during peak times. For the database, using Amazon RDS with Multi-AZ deployment provides a managed, highly available database solution that requires minimal administrative effort.

738. Question #844A 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?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Windows File Server
- C. AWS Snowball
- D. AWS Storage Gateway**

答案: D

解析: Given the requirement for low-latency access and the inability to modify the application code, AWS Storage Gateway is the recommended service. It allows on-premises applications to use AWS cloud storage services seamlessly by keeping the presentation layer consistent and utilizing the existing SMB protocol.

解析: Given the requirement for low-latency access and the inability to modify the application code, AWS Storage Gateway is the recommended service. It allows on-premises applications to use AWS cloud storage services seamlessly by keeping the presentation layer consistent and utilizing the existing SMB protocol.

739. Question #845A 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?**

- 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.

答案：C

解析：The most operationally efficient solution is to use AWS Lambda in combination with Amazon SNS. Lambda functions can be triggered automatically to scan the DynamoDB table and send out emails without the need for managing servers or running background jobs on EC2 instances.

解析：The most operationally efficient solution is to use AWS Lambda in combination with Amazon SNS. Lambda functions can be triggered automatically to scan the DynamoDB table and send out emails without the need for managing servers or running background jobs on EC2 instances.

740. Question #846A 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?

- 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.

答案：B

解析：To proactively handle the anticipated increase in traffic, a scheduled action in the Auto Scaling group should be set up to scale up before the holiday period. This ensures that the system is prepared to handle the load without waiting for utilization-based triggers.

解析：To proactively handle the anticipated increase in traffic, a scheduled action in the Auto Scaling group should be set up to scale up before the holiday period. This ensures that the system is prepared to handle the load without waiting for utilization-based triggers.

741. Question #847A 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**?

- 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.

答案：A

解析：Using AWS Secrets Manager is the most straightforward solution for managing and rotating database credentials. It is designed to handle secrets and automatically rotate them with minimal configuration and effort.

解析：Using AWS Secrets Manager is the most straightforward solution for managing and rotating database credentials. It is designed to handle secrets and automatically rotate them with minimal configuration and effort.

742. Question #848A 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?

- 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.

答案：B

解析：To maintain the use of third-party features and privileged access while benefiting from the BYOL model, migrating to Amazon RDS Custom for Oracle is the most cost-effective solution. This allows for the necessary customization and the use of existing Oracle licenses.

解析: To maintain the use of third-party features and privileged access while benefiting from the BYOL model, migrating to Amazon RDS Custom for Oracle is the most cost-effective solution. This allows for the necessary customization and the use of existing Oracle licenses.

743. Question #849A 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?

- 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.

答案: B

解析: AWS Backup is a centralized service that can automate and manage backups across various AWS services such as Amazon EC2, Amazon RDS, and Amazon DynamoDB. It is the native AWS solution designed for this purpose.

解析: AWS Backup is a centralized service that can automate and manage backups across various AWS services such as Amazon EC2, Amazon RDS, and Amazon DynamoDB. It is the native AWS solution designed for this purpose.

744. Question #850A 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?

- 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.

答案: B

解析: Amazon Neptune is a graph database designed to store and query relationships, making it ideal for mapping IT infrastructure. SPARQL is a query language for graph databases that allows for complex queries to identify security risks efficiently.

解析: Amazon Neptune is a graph database designed to store and query relationships, making it ideal for mapping IT infrastructure. SPARQL is a query language for graph databases that allows for complex queries to identify security risks efficiently.

745. Question #851A 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**. Which solution will meet these requirements **MOST cost-effectively**?

- 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.

答案: C

解析: Amazon Aurora Serverless is a cost-effective solution for developers who only need databases during active development periods. It automatically scales with the application's needs and charges for only the capacity used.

解析: Amazon Aurora Serverless is a cost-effective solution for developers who only need databases during active development periods. It automatically scales with the application's needs and charges for only the capacity used.

746. Question #852A 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?

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.

答案：B

解析：Amazon EFS is designed to provide a shared file system that can be accessed by multiple EC2 instances simultaneously. By mounting EFS to each instance, the website assets remain consistent across all instances with minimal lag.

解析：Amazon EFS is designed to provide a shared file system that can be accessed by multiple EC2 instances simultaneously. By mounting EFS to each instance, the website assets remain consistent across all instances with minimal lag.

747. Question #853A 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?

- 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.

答案：A

解析: Amazon GuardDuty is specifically designed for threat detection. By integrating it with Amazon EventBridge and AWS Lambda, the system can automatically adjust AWS WAF rules in response to detected threats, providing a robust defense mechanism.

解析: Amazon GuardDuty is specifically designed for threat detection. By integrating it with Amazon EventBridge and AWS Lambda, the system can automatically adjust AWS WAF rules in response to detected threats, providing a robust defense mechanism.

748. Question #854A 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?

- 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.

答案: C

解析: IAM database authentication allows the EC2 instances to connect to the Aurora database using IAM roles, which can be managed and rotated without the need for handling static credentials. This method reduces

operational effort and enhances security.

解析: IAM database authentication allows the EC2 instances to connect to the Aurora database using IAM roles, which can be managed and rotated without the need for handling static credentials. This method reduces operational effort and enhances security.

749. Question #855A 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?**

- 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.

答案: C

解析: AWS Certificate Manager (ACM) provides free SSL/TLS certificates for public domain names. By requesting a public certificate, the company can use a custom domain name for its CloudFront distribution without additional costs.

解析: AWS Certificate Manager (ACM) provides free SSL/TLS certificates for public domain names. By requesting a public certificate, the company can use a custom domain name for its CloudFront distribution without additional costs.

750. Question #856A 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**?

- 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.**

答案：D

解析：A presigned URL provides time-limited access to a specific object in the S3 bucket without giving the external consultant access to the entire bucket or requiring long-term credentials. This method is the most operationally efficient and secure.

解析：A presigned URL provides time-limited access to a specific object in the S3 bucket without giving the external consultant access to the entire bucket or requiring long-term credentials. This method is the most operationally efficient and secure.

751. Question #857A 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?

- 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.

答案：A

解析: Cluster placement groups are designed for HPC workloads that need low-latency, high-throughput networking. They group instances closely together inside an Availability Zone, which is ideal for tightly coupled node-to-node communication.

解析: Cluster placement groups are designed for HPC workloads that need low-latency, high-throughput networking. They group instances closely together inside an Availability Zone, which is ideal for tightly coupled node-to-node communication.

752. Question #858A 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?

- 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

答案: C

解析: To achieve maximum resiliency, the solution should include multiple connections from each data center to separate Direct Connect locations. This ensures that there is redundancy in case one connection or location fails.

解析: To achieve maximum resiliency, the solution should include multiple connections from each data center to separate Direct Connect locations.

This ensures that there is redundancy in case one connection or location fails.

753. Question #860A 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?

- 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 VPC. In 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.

答案：A

解析：A gateway endpoint for Amazon S3 allows private connections between the VPC and S3, which minimizes data transfer costs by avoiding internet traffic. This is the most cost-effective solution for frequent access to large S3 files.

解析：A gateway endpoint for Amazon S3 allows private connections between the VPC and S3, which minimizes data transfer costs by avoiding internet traffic. This is the most cost-effective solution for frequent access to large S3 files.

754. Question #861A 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?

- 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.

答案：A

解析：To address the high volume of write operations and potential performance issues, a Provisioned IOPS SSD storage option for the Amazon RDS MySQL DB instance is recommended. This provides consistent and high-performance storage that can be adjusted as needed based on CloudWatch metrics.

解析：To address the high volume of write operations and potential performance issues, a Provisioned IOPS SSD storage option for the Amazon RDS MySQL DB instance is recommended. This provides consistent and high-performance storage that can be adjusted as needed based on CloudWatch metrics.

755. Question #862A 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?

- 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.

答案: D

解析: To ensure that third parties do not have access to the data before it is encrypted, client-side encryption with a key stored in AWS KMS is the appropriate solution. This allows the application to encrypt data locally before sending it to the S3 bucket.

解析: To ensure that third parties do not have access to the data before it is encrypted, client-side encryption with a key stored in AWS KMS is the appropriate solution. This allows the application to encrypt data locally before sending it to the S3 bucket.

756. Question #863A 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?

- 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.

答案：B

解析：Modifying the RDS database settings to include a 30-day retention period for automated backups is the simplest and most operationally efficient way to meet the regulatory requirements without additional overhead.

解析：Modifying the RDS database settings to include a 30-day retention period for automated backups is the simplest and most operationally efficient way to meet the regulatory requirements without additional overhead.

757. Question #864A 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?

- 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.

答案：C

解析：Creating an Aurora read replica is the most cost-effective way to increase scalability for read-heavy workloads. It allows the read queries to be distributed to the replica while write operations are handled by the primary cluster.

解析: Creating an Aurora read replica is the most cost-effective way to increase scalability for read-heavy workloads. It allows the read queries to be distributed to the replica while write operations are handled by the primary cluster.

758. Question #867A 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?
- 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.

答案: D

解析: AWS Compute Optimizer provides recommendations on the right EC2 instance types and EBS volume sizes based on the usage and performance patterns. It helps in optimizing costs by suggesting the most cost-effective resources, which includes EBS volume optimization.

解析: AWS Compute Optimizer provides recommendations on the right EC2 instance types and EBS volume sizes based on the usage and performance patterns. It helps in optimizing costs by suggesting the most cost-effective resources, which includes EBS volume optimization.

759. Question #868*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?

- A. 缺失A答案，待补齐
- B. Enable IAM Access Analyzer for S3 to identify all S3 buckets that are not versioning-enabled across Regions.
- C. Enable AWS Config 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.

答案: B

解析: waiting....

解析: waiting....

760. Question #869A company wants to enhance its e-commerce 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?

- 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.

答案: A

解析: Amazon SQS FIFO (First-In-First-Out) queues are designed to ensure that each message (order) is processed exactly once. By triggering an AWS Lambda function for each message, the system can scale and maintain order integrity during traffic surges without affecting the customer experience.

解析: Amazon SQS FIFO (First-In-First-Out) queues are designed to ensure that each message (order) is processed exactly once. By triggering an AWS Lambda function for each message, the system can scale and maintain order integrity during traffic surges without affecting the customer experience.

761. Question #870A 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?

- 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.**

答案: D

解析: old(B)-->new(D) old: Creating an IAM role in the Development account and granting it access to the Production account allows developers to assume the role when necessary. This provides a secure and flexible way to manage access between accounts, especially as requirements change during different phases of development.

解析: old(B)-->new(D) old: Creating an IAM role in the Development account and granting it access to the Production account allows developers to assume the role when necessary. This provides a secure and flexible way to manage access between accounts, especially as requirements change during different phases of development.

762. Question #871A 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?

- 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.

答案：A

解析：Amazon Cognito is a fully managed service that provides authentication and user directory services. Lambda@Edge can be used for serverless authorization, and Amazon CloudFront can distribute and cache content globally to provide low-latency access to users worldwide.

解析：Amazon Cognito is a fully managed service that provides authentication and user directory services. Lambda@Edge can be used for serverless authorization, and Amazon CloudFront can distribute and cache content globally to provide low-latency access to users worldwide.

763. Question #872A 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?

- 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 E02 instances, and apply it to the AWS accounts.

答案：D

解析：By creating a service control policy (SCP) within an AWS Organization, thesolutions architect can set restrictions that apply to all accounts within the organization. This is a centralized approach that requires less operational overhead compared to individually updating policies or roles in each account.

解析：By creating a service control policy (SCP) within an AWS Organization, thesolutions architect can set restrictions that apply to all accounts within the organization. This is a centralized approach that requires less operational overhead compared to individually updating policies or roles in each account.

764. Question #873A 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?

- 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.

答案: B

解析: Based on the company's requirements to automate inventory and updates of operating systems for a diverse fleet of EC2 instances running Windows Server and Linux distributions, as well as the need for monthly vulnerability summaries, I recommend the following solution: B. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Deploy Amazon Inspector, and configure monthly reports. Here's a breakdown of this recommendation:

- 1. AWS Systems Manager Patch Manager:
 - Automates the process of patching and updating operating systems across the fleet of EC2 instances.
 - Supports both Windows Server and Linux distributions.
 - Provides centralized control and reporting for patch compliance.
 - Allows for scheduling and automation of patching activities.
- 2. Amazon Inspector:
 - Automatically assesses EC2 instances for vulnerabilities and deviations from best practices.
 - Provides detailed reports on common vulnerabilities and exposures (CVEs).
 - Supports both Windows and Linux operating systems.
 - Can be configured to generate monthly reports for regular reviews.

Implementation steps and best practices:

- 1. Set up AWS Systems Manager:
 - Install the SSM Agent on all EC2 instances if not already present.
 - Configure appropriate IAM roles and permissions for Systems Manager to access the instances.
- 2. Configure Patch Manager:
 - Create patch baselines for different operating systems.
 - Set up patch groups to organize instances.
 - Schedule patching operations during maintenance windows to minimize disruption.
- 3. Deploy Amazon Inspector:
 - Enable Amazon Inspector in your AWS account.
 - Install the Amazon Inspector agent on all EC2 instances.
 - Configure assessment targets and templates.
- 4. Set up monthly reporting:
 - Use Amazon Inspector's built-in reporting features to generate monthly vulnerability summaries.

- Consider integrating with Amazon CloudWatch Events to automate report generation and distribution.
- 5. Security best practices:
 - Follow the principle of least privilege when configuring IAM roles for Systems Manager and Inspector.
 - Regularly review and update patch baselines to include the latest security patches.
 - Implement a process to review and act on the vulnerability reports generated by Amazon Inspector.
- 6. Additional considerations:
 - Use AWS Config to maintain an inventory of EC2 instances and track configuration changes.
 - Consider implementing AWS Security Hub for a comprehensive view of your security posture across AWS accounts. By implementing this solution, the company can effectively automate OS updates, maintain an inventory of instances, and receive regular vulnerability assessments, meeting their stated requirements for managing their diverse fleet of EC2 instances.

Sources [1] [Amazon EC2 instances – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html>) [3] [Amazon Elastic Compute Cloud (EC2) Instances – Developing and Deploying .NET Applications on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/amazon-elastic-compute-cloud-ec2-instances.html>) [6] [Update management for Amazon EC2 instances – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/update-management.html>)

解析: Based on the company's requirements to automate inventory and updates of operating systems for a diverse fleet of EC2 instances running Windows Server and Linux distributions, as well as the need for monthly vulnerability summaries, I recommend the following solution:

B. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Deploy Amazon Inspector, and configure monthly reports. Here's a breakdown of this recommendation:

1. AWS Systems Manager Patch Manager:
 - Automates the process of patching and updating operating systems across the fleet of EC2 instances.
 - Supports both Windows Server and Linux distributions.
 - Provides centralized control and reporting for patch compliance.
 - Allows for scheduling and automation of patching activities.
2. Amazon Inspector:
 - Automatically assesses EC2 instances for vulnerabilities and deviations from best practices.

Provides detailed reports on common vulnerabilities and exposures (CVEs).

– Supports both Windows and Linux operating systems. – Can be configured to generate monthly reports for regular reviews.

Implementation steps and best practices:

1. Set up AWS Systems Manager:
 - Install the SSM Agent on all EC2 instances if not already present.
 - Configure appropriate IAM roles and permissions for Systems Manager to access the instances.
2. Configure Patch Manager:
 - Create patch baselines for different operating systems.
 - Set up patch groups to organize instances.
 - Schedule patching operations during maintenance windows to minimize disruption.
3. Deploy Amazon Inspector:
 - Enable Amazon Inspector in your AWS account.
 - Install the Amazon Inspector agent on all EC2 instances.
 - Configure assessment targets and templates.
4. Set up monthly reporting:
 - Use Amazon Inspector's built-in reporting features to generate monthly vulnerability summaries.

- Consider integrating with Amazon CloudWatch Events to automate report generation and distribution.
5. Security best practices:
 - Follow the principle of least privilege when configuring IAM roles for Systems Manager and Inspector.
 - Regularly review and update patch baselines to include the latest security patches.
 - Implement a process to review and act on the vulnerability reports generated by Amazon Inspector.
6. Additional considerations:
 - Use AWS Config to maintain an inventory of EC2 instances and track configuration changes.

- Consider implementing AWS Security Hub for a comprehensive view of your security posture across AWS accounts. By implementing this solution, the company can effectively automate OS updates, maintain an inventory of instances, and receive regular vulnerability assessments, meeting their stated requirements for managing their diverse fleet of EC2 instances.

Sources [1] [Amazon EC2 instances – Amazon Elastic Compute Cloud]

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html>) [3]

[Amazon Elastic Compute Cloud (EC2) Instances – Developing and Deploying .NET Applications on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/amazon-elastic-compute-cloud-ec2-instances.html>) [6]

[Update management for Amazon EC2 instances – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/>

de/update-management.html)

765. Question #874A 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?

- 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.

答案：A

解析：By pre-configuring an Auto Scaling group and ELB in the DR Region and setting up the DynamoDB table as a global table, the company can quickly switch traffic to the DR Region using DNS failover. This approach minimizes downtime as it does not require on-demand infrastructure setup during a disaster.

解析：By pre-configuring an Auto Scaling group and ELB in the DR Region and setting up the DynamoDB table as a global table, the company can quickly switch traffic to the DR Region using DNS failover. This approach minimizes downtime as it does not require on-demand infrastructure setup during a disaster.

766. Question #875A 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?

- 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.

答案：D

解析：An S3 gateway endpoint provides the most cost-effective solution for allowing private access to S3 buckets from within a VPC. It does not require additional infrastructure like a NAT gateway or AWS Storage Gateway and does not incur data transfer costs over the public internet.

解析：An S3 gateway endpoint provides the most cost-effective solution for allowing private access to S3 buckets from within a VPC. It does not require additional infrastructure like a NAT gateway or AWS Storage Gateway and does not incur data transfer costs over the public internet.

767. Question #877A 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?

- 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.

答案：B

解析：Using Amazon API Gateway and AWS Lambda provides a serverless solution for handling form submissions and sending notifications. This approach is cost-effective, especially for a low-volume website, as it scales with usage and requires no ongoing management.

解析：Using Amazon API Gateway and AWS Lambda provides a serverless solution for handling form submissions and sending notifications. This approach is cost-effective, especially for a low-volume website, as it scales with usage and requires no ongoing management.

768. Question #878A 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?

- 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.

答案：B

解析：Configuring each AWS account to use a unique email distribution list for each business unit allows for targeted notifications based on the category. This approach enhances security by ensuring that only the relevant team members receive sensitive notifications and can respond to alerts.

解析：Configuring each AWS account to use a unique email distribution list for each business unit allows for targeted notifications based on the category. This approach enhances security by ensuring that only the relevant team members receive sensitive notifications and can respond to alerts.

769. Question #880A 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?

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.

答案：B

解析：Amazon Athena allows direct querying of data in S3 using SQL, making it a suitable choice for analyzing the AWS Cost and Usage Report stored in S3. Amazon QuickSight can then be used to create a custom dashboard based on the Athena query results, providing an easy-to-understand visualization for senior leadership.

解析：Amazon Athena allows direct querying of data in S3 using SQL, making it a suitable choice for analyzing the AWS Cost and Usage Report stored in S3. Amazon QuickSight can then be used to create a custom dashboard based on the Athena query results, providing an easy-to-understand visualization for senior leadership.

770. Question #882A 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?

- 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.

答案: C

解析: A Compute Savings Plan offers significant discounts on both EC2 and Lambda usage compared to on-demand pricing. By connecting Lambda functions to private subnets, the company ensures direct network access to the EC2 instances, which is necessary for the application to work effectively while keeping costs minimized.

解析: A Compute Savings Plan offers significant discounts on both EC2 and Lambda usage compared to on-demand pricing. By connecting Lambda functions to private subnets, the company ensures direct network access to the EC2 instances, which is necessary for the application to work effectively while keeping costs minimized.

771. Question #208A 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?

- 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.

答案：A

解析：答案应该是A，请自行确认。

解析：答案应该是A，请自行确认。

772. Question#232A 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.

- 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.

答案：C

773. Question#234A 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?

- 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.

答案：C

774. Question#235A 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?

- 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.

答案：C

775. Question#236A 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?

- 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.

答案：D

776. Question#237An 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?

- 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.

答案：A

777. Question #883A 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?

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.

答案：B

解析：To implement controls to limit AWS resource costs for developers in a multi-account strategy using AWS Control Tower, the solution with the least operational overhead is: 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.

1. Set up AWS Budgets
 - Navigate to the AWS Budgets console
 - Create a budget for each developer account
 - Set appropriate budget amounts based on company policies
2. Configure Budget Alerts
 - Set up alerts for actual and forecasted spend
 - Define thresholds (e.g., 80%, 90%, 100% of budget)
 - Configure email notifications for developers and administrators
3. Implement AWS Budgets Actions
 - Create a DenyAll IAM policy
 - Configure Budgets Actions to apply this policy when the budget is reached
 - Ensure the action targets the developer's IAM role
4. Test and Verify
 - Simulate budget exceedance to ensure alerts and actions work as expected
 - Verify that developers receive notifications and resource creation is blocked when the budget is reached
5. Monitor and Adjust
 - Regularly review budget utilization across accounts
 - Adjust budgets and thresholds as needed based on business requirements

This solution provides automated cost control with minimal operational overhead. It allows developers to monitor their own spending while providing an automatic mechanism to prevent overspending. Remember to review and adjust the budgets periodically to ensure they align with business needs and cost optimization goals.

Sources [1] [Cost-effective resources – AWS Well-Architected Framework (2022-03-31)] (<https://docs.aws.amazon.com/wellarchitected/2022-03-31/framework/cost-cereso.html>) [3] [Cost-effective resources – AWS Well-Architected Framework] (<https://docs.aws.amazon.com/wellarchitected/latest/framework/cost-cereso.html>) [6] [Cost-effective resources – AWS Well-Architected Framework] (<https://docs.aws.amazon.com/wellarchitected/2024-06-27/framework/cost-cereso.html>)

解析: To implement controls to limit AWS resource costs for developers in a multi-account strategy using AWS Control Tower, the solution with the least operational overhead is:

- 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.

1. Set up AWS Budgets – Navigate to the AWS Budgets console
- Create a budget for each developer account
- Set appropriate budget amounts based on company policies
2. Configure Budget Alerts – Set up alerts for actual and forecasted spend
- Define thresholds (e.g., 80%, 90%, 100% of budget)
- Configure email notifications for developers and administrators
3. Implement AWS Budgets Actions – Create a DenyAll IAM policy
- Configure Budgets Actions to apply this policy when the budget is reached
- Ensure the action targets the developer's IAM role
4. Test and Verify – Simulate budget exceedance to ensure alerts and actions work as expected
- Verify that developers receive notifications and resource creation is blocked when the budget is reached
5. Monitor and Adjust – Regularly review budget utilization across accounts
- Adjust budgets and thresholds as needed based on business requirements

This solution provides automated cost control with minimal operational overhead. It allows developers to monitor their own spending while providing an automatic mechanism to prevent overspending. Remember to review and adjust the budgets periodically to ensure they align with business needs and cost optimization goals.

Sources [1] [Cost-effective resources – AWS Well-Architected Framework (2022-03-31)] (<https://docs.aws.amazon.com/wellarchitected/2022-03-31/framework/cost-cereso.html>) [3] [Cost-effective resources – AWS Well-Architected Framework] (<https://docs.aws.amazon.com/wellarchitected/latest/framework/cost-cereso.html>) [6] [Cost-effective resources – AWS Well-Architected Framework] (<https://docs.aws.amazon.com/wellarchitected/2024-06-27/framework/cost-cereso.html>)

778. Question #887A 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?

- 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.

答案：B

解析：The correct solution is B. Using AWS Config to identify and ensure all EBS volumes are encrypted by default and applying a default AWS KMS key for encryption meets the requirement of ensuring all new EBS volumes are encrypted and prevents the creation of unencrypted volumes. Option A is incorrect because it only sets the account attribute to encrypt EBS volumes but does not ensure it or prevent unencrypted volume creation. Options C and D do not address the prevention of unencrypted volume creation.

解析：The correct solution is B. Using AWS Config to identify and ensure all EBS volumes are encrypted by default and applying a default AWS KMS key for encryption meets the requirement of ensuring all new EBS volumes are encrypted and prevents the creation of unencrypted volumes. Option A is incorrect because it only sets the account attribute to encrypt EBS volumes but does not ensure it or prevent unencrypted volume creation. Options C and D do not address the prevention of unencrypted volume creation.

779. Question #888 An e-commerce 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?

- 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.

答案：A

解析：The correct solution is A. Amazon Kinesis Data Streams with on-demand mode can automatically scale to handle varying levels of traffic without the need for manual intervention, making it a cost-effective choice for fluctuating traffic. Using AWS Lambda for real-time processing complements this by providing a serverless compute solution. Option B is less suitable because AWS Glue is not designed for real-time processing. Option C is incorrect because Amazon Kinesis Video Streams is for video data, not clickstream data. Option D, while capable, combines services that are not as cost-effective for this specific use case as the combination of Kinesis Data Streams and Lambda.

解析：The correct solution is A. Amazon Kinesis Data Streams with on-demand mode can automatically scale to handle varying levels of traffic without the need for manual intervention, making it a cost-effective choice for fluctuating traffic. Using AWS Lambda for real-time processing complements this by providing a serverless compute solution. Option B is less suitable because AWS Glue is not designed for real-time processing. Option C is incorrect because Amazon Kinesis Video Streams is for video data, not clickstream data. Option D, while capable, combines services that are not as cost-effective for this specific use case as the combination of Kinesis Data Streams and Lambda.

780. Question #889A 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?

- 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.

答案：B

解析：To identify all S3 buckets that are not versioning-enabled across AWS Regions for a global company, the recommended solution is: B. Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions. Here's a step-by-step guide to implement this solution:

1. Enable Amazon S3 Storage Lens – Navigate to the Amazon S3 console. – In the left navigation pane, select "Storage Lens". – Click "Create dashboard" if you haven't set one up already.
2. Configure S3 Storage Lens dashboard – Choose a dashboard name and select the scope (organization-wide or specific accounts/regions). – Enable advanced metrics and recommendations. – In the "Select metrics" section, ensure "Versioning" is selected.
3. Set up data export (optional but recommended) – Configure S3 Storage Lens to export detailed data to an S3 bucket for further analysis.
4. Create a filter for non-versioned buckets – Once your dashboard is active, navigate to the "Buckets" tab. – Use the filter option to show only buckets where "Versioning enabled" is "No".
5. Review and analyze the results – Examine the list of buckets that do not have versioning enabled. – You can export this data for further analysis or action.
6. Enable versioning on identified buckets – For each bucket identified, navigate to its properties in the S3 console. – Under the "Versioning" section, choose "Enable versioning".
7. Set up ongoing monitoring – Use S3 Storage Lens dashboards regularly to monitor versioning status across your buckets. – Consider setting up alerts or automated reports

to stay informed about non-versioned buckets. This approach allows you to efficiently identify and address non-versioned buckets across your global AWS infrastructure. S3 Storage Lens provides a comprehensive view of your S3 usage and can help you implement data protection best practices.

Sources [1] [Retaining multiple versions of objects with S3 Versioning – Amazon Simple Storage Service]

(<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>)

[3] [Identify public S3 buckets in AWS Organizations using Security Hub – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/identify-public-s3-buckets-in-aws-organizations-using-security-hub.html>) [6] [Using S3 Storage Lens to protect your data – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-lens-data-protection.html>)

解析: To identify all S3 buckets that are not versioning-enabled across AWS Regions for a global company, the recommended solution is: B. Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions. Here's a step-by-step guide to implement this solution:

1. Enable Amazon S3 Storage Lens – Navigate to the Amazon S3 console. – In the left navigation pane, select "Storage Lens". – Click "Create dashboard" if you haven't set one up already.
2. Configure S3 Storage Lens dashboard – Choose a dashboard name and select the scope (organization-wide or specific accounts/regions). – Enable advanced metrics and recommendations. – In the "Select metrics" section, ensure "Versioning" is selected.
3. Set up data export (optional but recommended) – Configure S3 Storage Lens to export detailed data to an S3 bucket for further analysis.
4. Create a filter for non-versioned buckets – Once your dashboard is active, navigate to the "Buckets" tab. – Use the filter option to show only buckets where "Versioning enabled" is "No".
5. Review and analyze the results – Examine the list of buckets that do not have versioning enabled.
6. Enable versioning on identified buckets – You can export this data for further analysis or action.
7. Set up ongoing monitoring – For each bucket identified, navigate to its properties in the S3 console. – Under the "Versioning" section, choose "Enable versioning".
8. Set up ongoing monitoring – Under the "Versioning" section, choose "Enable versioning".

Use S3 Storage Lens dashboards regularly to monitor versioning status across your buckets. – Consider setting up alerts or automated reports to stay informed about non-versioned buckets. This approach allows you to efficiently identify and address non-versioned buckets across your global AWS infrastructure. S3 Storage Lens provides a comprehensive view of your S3 usage and can help you implement data protection best practices.

Sources [1] [Retaining multiple versions of objects with S3 Versioning – Amazon Simple Storage Service]

(<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html>)

[3] [Identify public S3 buckets in AWS Organizations using Security Hub – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/identify-public-s3-buckets-in-aws-organizations-using-security-hub.html>) [6] [Using S3 Storage Lens to protect your data – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-lens-data-protection.html>)

781. Question #890A 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?**

- 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.

答案：C

解析：Based on the company's requirements for optimizing S3 storage costs while maintaining immediate accessibility and considering the access patterns, the most cost-effective solution is: Option 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. Here's why this solution is the most suitable:

- 1. Initial storage: The files will remain in S3 Standard for the first 30 days, which is appropriate for the frequent access during this period.
- 2. Long-term storage: After 30 days, the files will be moved to S3 Standard-IA, which is designed for infrequently accessed data but still provides immediate access when needed.
- 3. Immediate accessibility: S3 Standard-IA maintains millisecond access, meeting the requirement for immediate accessibility throughout the 4-year retention period.
- 4. Cost-effectiveness: S3 Standard-IA offers lower storage costs compared to S3 Standard, making it more cost-effective for the long-term storage of rarely accessed files.
- 5. Durability and availability: S3 Standard-IA provides the same high durability and availability as S3 Standard, ensuring data integrity and accessibility.
- 6. Minimum file size requirement: The 5 MB file size meets the minimum object size requirement for S3 Standard-IA (128 KB), avoiding any additional charges for smaller objects.
- 7. Lifecycle management: The S3 Lifecycle policy will automatically handle the transition to S3 Standard-IA after 30 days and the deletion after 4 years, reducing manual management overhead.

To implement this solution:

1. Create an S3 Lifecycle policy for the bucket containing these files.
2. Configure the policy to transition objects to S3 Standard-IA 30 days after creation.
3. Set up an expiration rule to delete the objects 4 years after creation.

Remember to review and adjust the policy as needed, and always test in a non-production environment before applying to critical data. For the most up-to-date pricing

information and specific details about S3 storage classes, please refer to the official AWS S3 documentation. Sources [1] [Managing the lifecycle of objects – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>) [3] [Analyze access patterns and use the most cost-effective Amazon S3 storage class | AWS Storage Blog] (<https://aws.amazon.com/blogs/storage/analyze-access-patterns-and-use-the-most-cost-effective-amazon-s3-storage-class/>) [6] [Save on storage costs using Amazon S3]

(<https://aws.amazon.com/s3/cost-optimization/>)

解析: Based on the company's requirements for optimizing S3 storage costs while maintaining immediate accessibility and considering the access patterns, the most cost-effective solution is: Option 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. Here's why this solution is the most suitable:

- 1. Initial storage: The files will remain in S3 Standard for the first 30 days, which is appropriate for the frequent access during this period.
- 2. Long-term storage: After 30 days, the files will be moved to S3 Standard-IA, which is designed for infrequently accessed data but still provides immediate access when needed.
- 3. Immediate accessibility: S3 Standard-IA maintains millisecond access, meeting the requirement for immediate accessibility throughout the 4-year retention period.
- 4. Cost-effectiveness: S3 Standard-IA offers lower storage costs compared to S3 Standard, making it more cost-effective for the long-term storage of rarely accessed files.
- 5. Durability and availability: S3 Standard-IA provides the same high durability and availability as S3 Standard, ensuring data integrity and accessibility.
- 6. Minimum file size requirement: The 5 MB file size meets the minimum object size requirement for S3 Standard-IA (128 KB), avoiding any additional charges for smaller objects.
- 7. Lifecycle management: The S3 Lifecycle policy will automatically handle the transition to S3 Standard-IA after 30 days and the deletion after 4 years, reducing manual management overhead.

To implement this solution:

1. Create an S3 Lifecycle policy for the bucket containing these files.
2. Configure the policy to transition objects to

S3 Standard-IA 30 days after creation. 3. Set up an expiration rule to delete the objects 4 years after creation. Remember to review and adjust the policy as needed, and always test in a non-production environment before applying to critical data. For the most up-to-date pricing information and specific details about S3 storage classes, please refer to the official AWS S3 documentation. Sources [1] [Managing the lifecycle of objects – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>) [3] [Analyze access patterns and use the most cost-effective Amazon S3 storage class | AWS Storage Blog] (<https://aws.amazon.com/blogs/storage/analyze-access-patterns-and-use-the-most-cost-effective-amazon-s3-storage-class/>) [6] [Save on storage costs using Amazon S3] (<https://aws.amazon.com/s3/cost-optimization/>)

782. Question #891A 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?

- 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.

答案: D

解析: The correct solution is D. Using Multi-Region Access Points in an active-active configuration with a single global endpoint allows the application to send data to the nearest S3 bucket without public network

congestion and simplifies failover management. Option A requires managing two active Regions, which increases complexity. Option B's active-passive configuration does not meet the requirement for the least amount of management. Option C involves managing cross-account replication, which adds overhead.

解析：The correct solution is D. Using Multi-Region Access Points in an active-active configuration with a single global endpoint allows the application to send data to the nearest S3 bucket without public network congestion and simplifies failover management. Option A requires managing two active Regions, which increases complexity. Option B's active-passive configuration does not meet the requirement for the least amount of management. Option C involves managing cross-account replication, which adds overhead.

783. Question #892A 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?

- 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 Mitigation 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.

答案：C

解析：The correct solution is C. Creating an AMI of each application instance and launching two EC2 instances in separate Availability Zones ensures fault tolerance. Configuring a Network Load Balancer with these instances as targets provides high availability. Option A's Auto Scaling group with a minimum and maximum of one does not provide fault tolerance. Option B's hourly backup and disaster recovery process does not ensure real-time fault tolerance. Option D's ECS with Fargate requires changes to the application design, which is not allowed.

解析：The correct solution is C. Creating an AMI of each application instance and launching two EC2 instances in separate Availability Zones ensures fault tolerance. Configuring a Network Load Balancer with these instances as targets provides high availability. Option A's Auto Scaling group with a minimum and maximum of one does not provide fault tolerance. Option B's hourly backup and disaster recovery process does not ensure real-time fault tolerance. Option D's ECS with Fargate requires changes to the application design, which is not allowed.

784. Question #893A 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**?

- 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 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 using a transit gateway attachment.

答案：A

解析：Based on the company's requirements to isolate workloads, centrally manage networking components, and automatically apply security controls, the solution that will meet these requirements with the least operational overhead is: 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. Here's why this solution is the most suitable:

- 1. AWS Control Tower:
 - Provides automated account creation with built-in security controls (guardrails).
 - Offers a simplified way to set up and govern multiple accounts.
 - Implements best practices for account structure and security out of the box.
- 2. Centralized Networking:
 - Creating a dedicated networking account allows for centralized management of network resources.
 - A single VPC with both private and public subnets in the networking account provides a standardized network architecture.
- 3. AWS Resource Access Manager (AWS RAM):
 - Enables secure sharing of the VPC subnets across accounts.
 - Reduces the need to create and manage separate VPCs in each workload account.
- 4. Least Operational Overhead:
 - Control Tower automates much of the account setup and governance process.
 - Centralized networking reduces the effort required to manage and maintain network configurations across multiple accounts.
 - Subnet sharing via AWS RAM simplifies network management and reduces duplication of effort.

Best practices and considerations for implementing this solution:

1. Design a well-structured organizational unit (OU) hierarchy in AWS Organizations to align with your business needs and security requirements.
2. Implement strong identity and access management (IAM) policies to control access to

shared resources. 3. Use AWS CloudFormation StackSets to deploy consistent resources and policies across accounts. 4. Regularly review and update the guardrails and security controls provided by Control Tower to ensure they meet your evolving security needs. 5. Implement proper network segmentation and security group configurations in the shared VPC to maintain isolation between workloads. 6. Use AWS CloudTrail and AWS Config for centralized logging and compliance monitoring across all accounts. 7. Regularly assess and optimize the shared network architecture to ensure it meets the performance and security requirements of all workloads. By following this approach, the company can achieve workload isolation, centralized network management, and automated security controls with minimal operational overhead.

ref: [1] [SEC01-BP01 Separate workloads using accounts – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/latest/framework/sec_securely_operate_multi_accounts.html) [3] [SEC01-BP01 Separate workloads using accounts – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2024-06-27/framework/sec_securely_operate_multi_accounts.html) [6] [SEC01-BP01 Separate workloads using accounts – Security Pillar] (https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_securely_operate_multi_accounts.html)

解析: Based on the company's requirements to isolate workloads, centrally manage networking components, and automatically apply security controls, the solution that will meet these requirements with the least operational overhead is: 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. Here's why this solution is the most suitable:

- 1. AWS Control Tower:
 - Provides automated account creation with built-in security controls (guardrails).
 - Offers a simplified way to set up and govern multiple accounts.
 - Implements best practices for account structure and security out of the box.
- 2. Centralized Networking:
 - Creating a dedicated networking account allows for centralized management of network resources.
 - A single VPC with both private and public subnets in the networking account provides a

standardized network architecture.

3. AWS Resource Access Manager (AWS RAM):

- Enables secure sharing of the VPC subnets across accounts.
- Reduces the need to create and manage separate VPCs in each workload account.

4. Least Operational Overhead:

- Control Tower automates much of the account setup and governance process.
- Centralized networking reduces the effort required to manage and maintain network configurations across multiple accounts.
- Subnet sharing via AWS RAM simplifies network management and reduces duplication of effort.

Best practices and considerations for implementing this solution:

1. Design a well-structured organizational unit (OU) hierarchy in AWS Organizations to align with your business needs and security requirements.
2. Implement strong identity and access management (IAM) policies to control access to shared resources.
3. Use AWS CloudFormation StackSets to deploy consistent resources and policies across accounts.
4. Regularly review and update the guardrails and security controls provided by Control Tower to ensure they meet your evolving security needs.
5. Implement proper network segmentation and security group configurations in the shared VPC to maintain isolation between workloads.
6. Use AWS CloudTrail and AWS Config for centralized logging and compliance monitoring across all accounts.
7. Regularly assess and optimize the shared network architecture to ensure it meets the performance and security requirements of all workloads.

By following this approach, the company can achieve workload isolation, centralized network management, and automated security controls with minimal operational overhead.

ref: [1] [SEC01-BP01 Separate workloads using accounts – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/latest/framework/sec_securely_operate_multi_accounts.html) [3] [SEC01-BP01 Separate workloads using accounts – AWS Well-Architected Framework] (https://docs.aws.amazon.com/wellarchitected/2024-06-27/framework/sec_securely_operate_multi_accounts.html) [6] [SEC01-BP01 Separate workloads using accounts – Security Pillar] (https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_securely_operate_multi_accounts.html)

785. Question #894A 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?

- 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.

答案：A

解析：The correct solution is A. Moving the static content to an S3 bucket and using CloudFront as a content delivery network (CDN) reduces hosting costs and improves content delivery speed. S3 is designed for static website hosting, and CloudFront can efficiently distribute content globally. Option B's ElastiCache does not serve static content. Option C's Amplify is not as cost-effective for serving static content at scale. Option D's EC2 instances are unnecessary when using S3 and CloudFront.

解析：The correct solution is A. Moving the static content to an S3 bucket and using CloudFront as a content delivery network (CDN) reduces hosting costs and improves content delivery speed. S3 is designed for static website hosting, and CloudFront can efficiently distribute content globally. Option B's ElastiCache does not serve static content. Option C's Amplify is not as cost-effective for serving static content at scale. Option D's EC2 instances are unnecessary when using S3 and CloudFront.

786. Question #8951. 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?

- 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.

答案: D

解析: The correct solution is D. Amazon FSx for Windows File Server is a fully managed service that provides a file system accessible via the SMB protocol, reducing administrative overhead. Option A's Storage Gateway requires managing a hybrid infrastructure. Option B's Tape Gateway is not suitable for file sharing access. Option C requires managing an EC2 instance and the file share role, which adds overhead.

解析: The correct solution is D. Amazon FSx for Windows File Server is a fully managed service that provides a file system accessible via the SMB protocol, reducing administrative overhead. Option A's Storage Gateway requires managing a hybrid infrastructure. Option B's Tape Gateway is not suitable for file sharing access. Option C requires managing an EC2 instance and the file share role, which adds overhead.

787. Question #896A 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?

- 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.

答案：B

解析：The correct solution is B. Converting the Aurora cluster to an Aurora global database and configuring managed failover provides the most operational efficiency. Aurora global databases replicate data across Regions with minimal impact on performance and can be used for disaster recovery. Option A's read replica does not offer the same level of automation and performance for DR purposes. Option C's Cross-Region Replication requires manual setup and management. Option D's AWS DMS is not the most efficient solution for the DR scenario described.

解析：The correct solution is B. Converting the Aurora cluster to an Aurora global database and configuring managed failover provides the most operational efficiency. Aurora global databases replicate data across Regions with minimal impact on performance and can be used for disaster recovery. Option A's read replica does not offer the same level of automation and performance for DR purposes. Option C's Cross-Region Replication requires manual setup and management. Option D's AWS DMS is not the most efficient solution for the DR scenario described.

788. Question #8971. 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?

- 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.

答案：A

解析：The correct solution is A. Using AWS Fargate with Amazon ECS and EventBridge Scheduler allows for running containerized jobs on a schedule without managing the underlying server infrastructure. Fargate supports running stateful jobs that require more than 15 minutes of execution time. Option B's Lambda function has a maximum execution time of 15 minutes, which is insufficient. Option C's EC2 Spot Instances may be interrupted, which is not suitable for stateful jobs. Option D's DataSync is not designed for running data analysis jobs.

解析：The correct solution is A. Using AWS Fargate with Amazon ECS and EventBridge Scheduler allows for running containerized jobs on a schedule without managing the underlying server infrastructure. Fargate supports running stateful jobs that require more than 15 minutes of execution time. Option B's Lambda function has a maximum execution time of 15 minutes, which is insufficient. Option C's EC2 Spot Instances may be interrupted, which is not suitable for stateful jobs. Option D's DataSync is not designed for running data analysis jobs.

789. Question #898A 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?

- 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.

答案：C

解析: The correct solution is C. Amazon Security Lake is a purpose-built solution for centralizing security data from AWS environments, requiring minimal development effort. It automatically collects and organizes security data, providing a comprehensive view. Option A involves more development effort with AWS Lake Formation and Glue. Option B requires custom development of a Lambda function. Option D's AWS DMS is not the most efficient solution for collecting security data.

解析: The correct solution is C. Amazon Security Lake is a purpose-built solution for centralizing security data from AWS environments, requiring minimal development effort. It automatically collects and organizes security data, providing a comprehensive view. Option A involves more development effort with AWS Lake Formation and Glue. Option B requires custom development of a Lambda function. Option D's AWS DMS is not the most efficient solution for collecting security data.

790. Question #899A 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?

- 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 application VPCs. Add routes from the shared services VPC subnets to the application 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.

答案：D

解析：The correct solution is D. A transit gateway simplifies the network architecture by acting as a hub for all VPCs, reducing the administrative overhead of managing multiple connections and routes. Option A's software VPN tunnels and Option B's VPC peering would require more management as the number of applications grows. Option C's AWS Direct Connect would also require managing multiple connections, which is not as scalable.

解析：The correct solution is D. A transit gateway simplifies the network architecture by acting as a hub for all VPCs, reducing the administrative overhead of managing multiple connections and routes. Option A's software VPN tunnels and Option B's VPC peering would require more management as the number of applications grows. Option C's AWS Direct Connect would also require managing multiple connections, which is not as scalable.

791. Question #901A 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?

- 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.

答案：B

解析: The correct solution is B. Migrating to a Multi-AZ Amazon RDS for SQL Server provides high availability, data durability, and managed maintenance, which reduces operational overhead. Using AWS KMS for encryption adds an extra layer of security for sensitive data. Option A requires managing EC2 instances, which increases operational overhead. Option C's Amazon S3 and Macie are not designed for relational database workloads. Option D's DynamoDB is a NoSQL database service and does not meet the relational database requirements.

解析: The correct solution is B. Migrating to a Multi-AZ Amazon RDS for SQL Server provides high availability, data durability, and managed maintenance, which reduces operational overhead. Using AWS KMS for encryption adds an extra layer of security for sensitive data. Option A requires managing EC2 instances, which increases operational overhead. Option C's Amazon S3 and Macie are not designed for relational database workloads. Option D's DynamoDB is a NoSQL database service and does not meet the relational database requirements.

792. Question #902A 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?

- 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 host 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.

答案：A

解析：The correct solution is A. Creating an Auto Scaling group across two Availability Zones provides high availability. The Application Load Balancer (ALB) can distribute traffic to the EC2 instances and is compatible with AWS WAF for added security. Option B's placement group does not provide the same level of availability as an Auto Scaling group. Option C does not use an Auto Scaling group, which limits scalability and availability. Option D incorrectly suggests connecting WAF directly to an Auto Scaling group, which is not supported.

解析：The correct solution is A. Creating an Auto Scaling group across two Availability Zones provides high availability. The Application Load Balancer (ALB) can distribute traffic to the EC2 instances and is compatible with AWS WAF for added security. Option B's placement group does not provide the same level of availability as an Auto Scaling group. Option C does not use an Auto Scaling group, which limits scalability and availability. Option D incorrectly suggests connecting WAF directly to an Auto Scaling group, which is not supported.

793. Question #903A company manages a data lake in an Amazon S3 bucket that numerous applications access. 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?

- 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.

答案：A

解析：Based on the company's requirements to manage access to a data lake in an Amazon S3 bucket with unique prefixes for each application, while maintaining granular control and minimizing operational overhead, the best solution is: A. Create dedicated S3 access points and access point policies for each application. This solution offers several advantages:

1. Granular Control: S3 Access Points allow you to create unique access control policies for each application, providing fine-grained control over access to specific prefixes within the bucket.
2. Least Operational Overhead: Once set up, Access Points require minimal ongoing management compared to other options like replication or managing individual object ACLs.
3. Scalability: You can create up to 10,000 access points per Region in each of your AWS accounts, which should be sufficient for most use cases.
4. Simplified Management: Each access point can have its own policy, making it easier to manage permissions for multiple applications accessing the same bucket.
5. Network Controls: Access Points also allow you to restrict access to specific VPCs if needed, adding an extra layer of security.

To implement this solution:

1. Create a separate Access Point for each application that needs to access the data lake.
2. Configure each Access Point to allow access only to the specific prefix associated with the respective application.
3. Set up Access Point policies to grant the necessary permissions (e.g., read, write) for each application. This approach aligns with AWS best practices for managing access to shared datasets in S3, providing a balance between security, granularity, and ease of management.

Remember to follow the principle of least privilege when setting up the access point policies, granting only the permissions necessary for each application to perform its required tasks. Also, consider enabling S3 server access logging to monitor and audit access to your data lake. For the most up-to-date information on S3 Access Points, including any limitations or additional features, please refer to the official AWS documentation. Sources [1] [Amazon S3 Access Points – Amazon Web Services]

(<https://aws.amazon.com/s3/features/access-points/>) [3] [Managing access with S3 Access Grants – Amazon Simple Storage Service] (<https://docs.aws>.

amazon.com/AmazonS3/latest/userguide/access-grants.html) [6] [Access control in Amazon S3 – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-management.html>)

解析: Based on the company's requirements to manage access to a data lake in an Amazon S3 bucket with unique prefixes for each application, while maintaining granular control and minimizing operational overhead, the best solution is: A. Create dedicated S3 access points and access point policies for each application. This solution offers several advantages: 1. Granular Control: S3 Access Points allow you to create unique access control policies for each application, providing fine-grained control over access to specific prefixes within the bucket. 2. Least Operational Overhead: Once set up, Access Points require minimal ongoing management compared to other options like replication or managing individual object ACLs. 3. Scalability: You can create up to 10,000 access points per Region in each of your AWS accounts, which should be sufficient for most use cases. 4. Simplified Management: Each access point can have its own policy, making it easier to manage permissions for multiple applications accessing the same bucket. 5. Network Controls: Access Points also allow you to restrict access to specific VPCs if needed, adding an extra layer of security. To implement this solution: 1. Create a separate Access Point for each application that needs to access the data lake. 2. Configure each Access Point to allow access only to the specific prefix associated with the respective application. 3. Set up Access Point policies to grant the necessary permissions (e.g., read, write) for each application. This approach aligns with AWS best practices for managing access to shared datasets in S3, providing a balance between security, granularity, and ease of management. Remember to follow the principle of least privilege when setting up the access point policies, granting only the permissions necessary for each application to perform its required tasks. Also, consider enabling S3 server access logging to monitor and audit access to your data lake. For the most up-to-date information on S3 Access Points, including any limitations or additional features, please refer to the official AWS documentation. Sources [1] [Amazon S3 Access Points – Amazon Web Services]

(<https://aws.amazon.com/s3/features/access-points/>) [3] [Managing access with S3 Access Grants – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-grants.html>) [6] [Access control in Amazon S3 – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-management.html>)

794. Question #904A 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?

- 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.

答案: A

解析: The correct solution is A. Using S3 Event Notifications with an SQS queue and AWS Lambda provides a serverless and cost-effective way to process images as they are uploaded. Lambda can scale automatically to handle the workload, and SQS ensures that all messages are processed. Option B's EC2 Reserved Instances would require managing servers and may not be as cost-effective. Option C's ECS and Option D's Elastic Beanstalk

involve more complex setups and may not be as cost-effective for this use case.

解析：The correct solution is A. Using S3 Event Notifications with an SQS queue and AWS Lambda provides a serverless and cost-effective way to process images as they are uploaded. Lambda can scale automatically to handle the workload, and SQS ensures that all messages are processed. Option B's EC2 Reserved Instances would require managing servers and may not be as cost-effective. Option C's ECS and Option D's Elastic Beanstalk involve more complex setups and may not be as cost-effective for this use case.

795. Question #906A 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?

- 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).

答案：C

解析：建议选择C

解析：建议选择C

796. Question #907A 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?

- 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.

答案: C

解析: C – Creating a presigned URL for the template object and configuring the CloudFormation stack to use it allows for secure access to the template in the S3 bucket based on specific user requests. It follows security best practices as the URL is only valid for a limited time and can be controlled. (A) creating a gateway VPC endpoint may not be necessary for this specific requirement and could add complexity. (B) using an API Gateway REST API with the S3 bucket as the target is not the most straightforward solution. (D) allowing public access initially and then blocking it later is not a secure approach and goes against security best practices.

解析: C – Creating a presigned URL for the template object and configuring the CloudFormation stack to use it allows for secure access to the template in the S3 bucket based on specific user requests. It follows security best practices as the URL is only valid for a limited time and can be controlled. (A) creating a gateway VPC endpoint may not be necessary for this specific requirement and could add complexity. (B) using an API Gateway REST API with the S3 bucket as the target is not the most straightforward solution. (D) allowing public access initially and then blocking it later is not a secure approach and goes against security best practices.

797. Question #908A 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?

- 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.

答案：A

解析：A – By confirming the installation of SSM Agent, assigning the appropriate instance profile, using IAM Identity Center for console access, and using Systems Manager Session Manager for permissions assignment, this solution provides a secure and controlled way for the

external support engineers to access the necessary resources without compromising security. (B) providing local IAM user credentials through Systems Manager Session Manager may not be the best practice as it could potentially introduce security risks. (C) relying solely on SSH access and IP address ranges may not provide the same level of security and management as the other options. (D) using a bastion host adds an additional layer of complexity and may not be the most efficient solution in this case.

解析: A – By confirming the installation of SSM Agent, assigning the appropriate instance profile, using IAM Identity Center for console access, and using Systems Manager Session Manager for permissions assignment, this solution provides a secure and controlled way for the external support engineers to access the necessary resources without compromising security. (B) providing local IAM user credentials through Systems Manager Session Manager may not be the best practice as it could potentially introduce security risks. (C) relying solely on SSH access and IP address ranges may not provide the same level of security and management as the other options. (D) using a bastion host adds an additional layer of complexity and may not be the most efficient solution in this case.

798. Question #909A 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?

- 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.

答案：D

解析：D – Creating a read replica in the same Region (us-east-1) is a cost-effective solution to improve database performance. The read replica can handle the read requests for the reports, reducing the load on the primary database. (A) creating a cross-Region read replica may introduce additional latency and costs. (B) activating Multi-AZ deployment is more for high availability rather than specifically addressing performance issues during business hours. (C) using AWS DMS to replicate data to a new database may be more complex and costly than simply creating a read replica.

解析：D – Creating a read replica in the same Region (us-east-1) is a cost-effective solution to improve database performance. The read replica can handle the read requests for the reports, reducing the load on the primary database. (A) creating a cross-Region read replica may introduce additional latency and costs. (B) activating Multi-AZ deployment is more for high availability rather than specifically addressing performance issues during business hours. (C) using AWS DMS to replicate data to a new database may be more complex and costly than simply creating a read replica.

799. Question #910A 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?

- 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.

答案：B

解析：B – Enabling detailed monitoring on all EC2 instances and using Amazon CloudWatch metrics allows for real-time monitoring and analysis of the web application's performance with a granularity of no more than 2 minutes. This provides immediate insights into the application's behavior. (A) sending CloudWatch logs to Amazon Redshift and using QuickSight may not provide the required real-time analysis. (C) creating an AWS Lambda function to fetch logs adds complexity and may not be necessary. (D) sending logs to S3 and using Redshift and QuickSight may introduce additional latency and is not the most efficient solution for real-time performance analysis.

解析：B – Enabling detailed monitoring on all EC2 instances and using Amazon CloudWatch metrics allows for real-time monitoring and analysis of the web application's performance with a granularity of no more than 2 minutes. This provides immediate insights into the application's behavior. (A) sending CloudWatch logs to Amazon Redshift and using QuickSight may not provide the required real-time analysis. (C) creating an AWS Lambda function to fetch logs adds complexity and may not be necessary. (D) sending logs to S3 and using Redshift and QuickSight may introduce additional latency and is not the most efficient solution for real-time performance analysis.

800. Question #911A 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?

- 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.

答案: C

解析: C – Configuring an S3 event notification to invoke an AWS Lambda function is a cost-effective solution as Lambda functions are serverless and can be triggered automatically when a new photo is uploaded. The Lambda function can then generate the thumbnail and upload it to the second S3 bucket. (A) using an Amazon EMR cluster for this task is overkill and not cost-effective. (B) using a memory-optimized EC2 instance that is always on is more expensive than using Lambda. (D) S3 Storage Lens is primarily for storage analytics and may not be the best choice for this specific requirement.

解析: C – Configuring an S3 event notification to invoke an AWS Lambda function is a cost-effective solution as Lambda functions are serverless and can be triggered automatically when a new photo is uploaded. The Lambda function can then generate the thumbnail and upload it to the second S3 bucket. (A) using an Amazon EMR cluster for this task is overkill and not cost-effective. (B) using a memory-optimized EC2 instance that is always on is more expensive than using Lambda. (D) S3

Storage Lens is primarily for storage analytics and may not be the best choice for this specific requirement.

801. Question #912A 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?

- 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.

答案: D

解析: D – Enabling S3 Inventory and using an AWS Lambda function to filter and delete objects based on the inventory reports is a serverless solution that meets the requirements. The Lambda function can be invoked with S3 Batch Operations to efficiently delete the objects. (A) using an EC2 instance to run the script is not a serverless solution and may incur higher costs. (B) AWS Batch may not be the most appropriate choice for this specific task of deleting objects based on age. (C) provisioning an AWS Glue crawler and creating a script to delete objects is more complex and may not be as efficient as using Lambda and S3 Batch Operations.

解析: D – Enabling S3 Inventory and using an AWS Lambda function to filter and delete objects based on the inventory reports is a serverless solution that meets the requirements. The Lambda function can be invoked

with S3 Batch Operations to efficiently delete the objects. (A) using an EC2 instance to run the script is not a serverless solution and may incur higher costs. (B) AWS Batch may not be the most appropriate choice for this specific task of deleting objects based on age. (C) provisioning an AWS Glue crawler and creating a script to delete objects is more complex and may not be as efficient as using Lambda and S3 Batch Operations.

802. Question #913A 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?

- 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.

答案: C

解析: C – Creating individual IAM roles for each Lambda function and granting them access to the S3 bucket ensures that only the authorized Lambda functions can access the data. By assigning each IAM role as the Lambda execution role, the principle of least privilege is followed. (A) granting full S3 bucket access to all Lambda functions through a shared IAM role does not provide the necessary granular access control. (B) configuring the Lambda functions to run within a VPC and using VPC endpoint IP addresses for access control may be more complex and not as effective as using IAM roles. (D) configuring a bucket policy based on function ARNs may not provide the same level of granularity and control

as using individual IAM roles.

解析: C – Creating individual IAM roles for each Lambda function and granting them access to the S3 bucket ensures that only the authorized Lambda functions can access the data. By assigning each IAM role as the Lambda execution role, the principle of least privilege is followed. (A) granting full S3 bucket access to all Lambda functions through a shared IAM role does not provide the necessary granular access control. (B) configuring the Lambda functions to run within a VPC and using VPC endpoint IP addresses for access control may be more complex and not as effective as using IAM roles. (D) configuring a bucket policy based on function ARNs may not provide the same level of granularity and control as using individual IAM roles.

803. Question #914A 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?

- 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.

答案：B

解析：B – Using Amazon CloudFront and Amazon S3 for the static web frontend provides global availability and caching. Refactoring the microservices to use AWS Lambda functions accessed through Amazon API Gateway is a serverless and scalable approach. Migrating the MySQL database to Amazon RDS for MySQL ensures better manageability and availability. This solution requires less operational overhead compared to the other options. (A) using AWS Amplify may not be necessary, and migrating to an EC2 Reserved Instance for the database does not provide the same level of managed services as RDS. (C) using a Network Load Balancer for the Lambda functions may not be the most suitable choice. (D) using an Application Load Balancer for the Lambda functions and an EC2 Reserved Instance for the database is not the most efficient and scalable solution.

解析：B – Using Amazon CloudFront and Amazon S3 for the static web frontend provides global availability and caching. Refactoring the microservices to use AWS Lambda functions accessed through Amazon API Gateway is a serverless and scalable approach. Migrating the MySQL database to Amazon RDS for MySQL ensures better manageability and availability. This solution requires less operational overhead compared to the other options. (A) using AWS Amplify may not be necessary, and migrating to an EC2 Reserved Instance for the database does not provide the same level of managed services as RDS. (C) using a Network Load Balancer for the Lambda functions may not be the most suitable choice. (D) using an Application Load Balancer for the Lambda functions and an EC2 Reserved Instance for the database is not the most efficient and scalable solution.

804. Question #915A 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**?

- 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.

答案：C

解析：C – Deploying an Amazon ElastiCache for Redis cluster provides fast access to the data as Redis is an in - memory data store that offers low latency. It also ensures data persistence on disks, meeting the requirements of the gaming application. (A) using Amazon S3 with Amazon CloudFront may not provide the same level of fast access as ElastiCache. (B) creating EC2 instances in multiple Regions and storing data on them requires more management and may not be as efficient for fast access. (D) while Amazon ElastiCache for Memcached can also be used for caching, Redis is often a better choice for applications that require data persistence.

解析：C – Deploying an Amazon ElastiCache for Redis cluster provides fast access to the data as Redis is an in - memory data store that offers low latency. It also ensures data persistence on disks, meeting the requirements of the gaming application. (A) using Amazon S3 with Amazon CloudFront may not provide the same level of fast access as ElastiCache. (B) creating EC2 instances in multiple Regions and storing data on them requires more management and may not be as efficient for fast access. (D) while Amazon ElastiCache for Memcached can also be used for caching, Redis is often a better choice for applications that require data

persistence.

805. Question #916A 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?**

- 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.

答案：D

解析：D – Creating separate AWS KMS keys for each customer's data allows for individual encryption and meets the requirement of encrypting data separately for each customer. With granular access control and logging enabled, it provides the necessary security and compliance. This solution also has the least operational overhead compared to the other options.

(A) storing keys in an S3 bucket and enabling server – side encryption may not provide the same level of control and security as using KMS keys.
(B) deploying a hardware security appliance adds complexity and may not be the most efficient solution. (C) using a single KMS key to encrypt all data does not meet the requirement of encrypting data separately for each customer.

解析：D – Creating separate AWS KMS keys for each customer's data allows for individual encryption and meets the requirement of encrypting data separately for each customer. With granular access control and logging

enabled, it provides the necessary security and compliance. This solution also has the least operational overhead compared to the other options.

(A) storing keys in an S3 bucket and enabling server – side encryption may not provide the same level of control and security as using KMS keys.
(B) deploying a hardware security appliance adds complexity and may not be the most efficient solution. (C) using a single KMS key to encrypt all data does not meet the requirement of encrypting data separately for each customer.

806. Question #917A 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?

- 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.

答案：D

解析：D – Using an Application Load Balancer to manage web traffic ensures efficient distribution of incoming requests. Amazon EC2 Auto Scaling groups can automatically scale up or down based on the traffic, ensuring that there are enough resources to receive and process customer

orders. Amazon SQS is a reliable and scalable message queuing service that can store unprocessed orders, allowing the application to handle bursts of traffic without losing orders. Amazon RDS with a Multi - AZ deployment provides high availability and durability for storing processed customer orders. (A) using a NAT gateway is not the best choice for managing web traffic in this scenario. (B) using Amazon Redshift for storing orders may not be the most appropriate database for this type of application. (C) using a GWLB to capture and store unprocessed orders is not a common practice, and DynamoDB may not be the best choice for storing processed orders in this case.

解析: D – Using an Application Load Balancer to manage web traffic ensures efficient distribution of incoming requests. Amazon EC2 Auto Scaling groups can automatically scale up or down based on the traffic, ensuring that there are enough resources to receive and process customer orders. Amazon SQS is a reliable and scalable message queuing service that can store unprocessed orders, allowing the application to handle bursts of traffic without losing orders. Amazon RDS with a Multi - AZ deployment provides high availability and durability for storing processed customer orders. (A) using a NAT gateway is not the best choice for managing web traffic in this scenario. (B) using Amazon Redshift for storing orders may not be the most appropriate database for this type of application. (C) using a GWLB to capture and store unprocessed orders is not a common practice, and DynamoDB may not be the best choice for storing processed orders in this case.

807. Question #918A 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?

- 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.

答案: D

解析: Based on the requirements provided, the most cost-effective solution for migrating and storing the files is to: 1. Configure AWS DataSync to use S3 Glacier Instant Retrieval as the destination storage class when migrating the files from the on-premises system. 2. Set up an S3 lifecycle policy to transition the objects from S3 Glacier Instant Retrieval to S3 Glacier Flexible Retrieval after 1 year. 3. Configure the lifecycle policy to include a retention period of 7 years for objects in S3 Glacier Flexible Retrieval. This solution meets the requirements in the following ways: – Initial storage: S3 Glacier Instant Retrieval is suitable for the first year when the files need to be immediately available but are accessed infrequently (once or twice). This storage class offers millisecond retrieval times at a lower cost than S3 Standard. – Long-term archival: S3 Glacier Flexible Retrieval is appropriate for long-term archiving of data that doesn't require immediate access. It's more cost-effective than Glacier Instant Retrieval for data that doesn't need millisecond retrieval times. – Lifecycle management: Using an S3 lifecycle policy to automatically transition the

files after 1 year ensures cost optimization without manual intervention.

- Small file size consideration: With an average file size of 10 KB, it's more efficient to store the files individually rather than grouping them into larger objects. This approach maintains granular access to individual files.
- Cost-effectiveness: This solution provides a good balance between accessibility and cost savings, aligning with the access patterns described (immediate access in the first year, then long-term archival).
- Retention period: S3 Glacier Flexible Retrieval supports the 7-year retention requirement for archival storage. To implement this solution:
 1. Configure AWS DataSync to use S3 Glacier Instant Retrieval as the destination storage class.
 2. Set up an S3 lifecycle policy to transition objects from S3 Glacier Instant Retrieval to S3 Glacier Flexible Retrieval after 1 year.
 3. Configure the lifecycle policy to include a retention period of 7 years for objects in S3 Glacier Flexible Retrieval.Sources [1] [Online Data Transfer and Migration - AWS DataSync - Amazon Web Services]

(<https://aws.amazon.com/datasync/resources/>) [3] [Save on storage costs using Amazon S3] (<https://aws.amazon.com/s3/cost-optimization/>) [6] [Cost optimization - Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/cost-optimization.html>) 2024-12-31: 此题确认选择D，没有疑问，对于同学反馈应该选择C答案，请阅读参考文档[1]中的内容有说明。

解析: Based on the requirements provided, the most cost-effective solution for migrating and storing the files is to:

1. Configure AWS DataSync to use S3 Glacier Instant Retrieval as the destination storage class when migrating the files from the on-premises system.
2. Set up an S3 lifecycle policy to transition the objects from S3 Glacier Instant Retrieval to S3 Glacier Flexible Retrieval after 1 year.
3. Configure the lifecycle policy to include a retention period of 7 years for objects in S3 Glacier Flexible Retrieval.

This solution meets the requirements in the following ways:

- Initial storage: S3 Glacier Instant Retrieval is suitable for the first year when the files need to be immediately available but are accessed infrequently (once or twice). This storage class offers millisecond retrieval times at a lower cost than S3

Standard. – Long-term archival: S3 Glacier Flexible Retrieval is appropriate for long-term archiving of data that doesn't require immediate access. It's more cost-effective than Glacier Instant Retrieval for data that doesn't need millisecond retrieval times. – Lifecycle management: Using an S3 lifecycle policy to automatically transition the files after 1 year ensures cost optimization without manual intervention. – Small file size consideration: With an average file size of 10 KB, it's more efficient to store the files individually rather than grouping them into larger objects. This approach maintains granular access to individual files. – Cost-effectiveness: This solution provides a good balance between accessibility and cost savings, aligning with the access patterns described (immediate access in the first year, then long-term archival). – Retention period: S3 Glacier Flexible Retrieval supports the 7-year retention requirement for archival storage. To implement this solution: 1. Configure AWS DataSync to use S3 Glacier Instant Retrieval as the destination storage class. 2. Set up an S3 lifecycle policy to transition objects from S3 Glacier Instant Retrieval to S3 Glacier Flexible Retrieval after 1 year. 3. Configure the lifecycle policy to include a retention period of 7 years for objects in S3 Glacier Flexible Retrieval. Sources [1] [Online Data Transfer and Migration – AWS DataSync – Amazon Web Services]

(<https://aws.amazon.com/datasync/resources/>) [3] [Save on storage costs using Amazon S3] (<https://aws.amazon.com/s3/cost-optimization/>) [6] [Cost optimization – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/cost-optimization.html>) 2024-12-31: 此题确认选择D，没有疑问，对于同学反馈应该选择C答案，请阅读参考文档[1]中的内容有说明。

808. Question #919A 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?

- 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.

答案：A

解析：A – Adding more Provisioned IOPS SSD (io1) EBS volumes and creating an LVM stripe can improve storage performance by increasing the I/O capacity and distributing the workload across multiple volumes. This can help address the performance issues compared to the on-premises database. (B) increasing the IOPS of the existing volume may not necessarily improve performance as it may still be limited by the single volume. (C) increasing the size of the volume alone does not directly address the performance problem. (D) changing the instance type to a storage optimized one may not be sufficient if the I/O capacity of the EBS volume is the bottleneck.

解析：A – Adding more Provisioned IOPS SSD (io1) EBS volumes and creating an LVM stripe can improve storage performance by increasing the I/O capacity and distributing the workload across multiple volumes. This can help address the performance issues compared to the on-premises database. (B) increasing the IOPS of the existing volume may not necessarily improve performance as it may still be limited by the single volume. (C) increasing the size of the volume alone does not directly address the performance problem. (D) changing the instance type to a storage optimized one may not be sufficient if the I/O capacity of the EBS volume is the bottleneck.

809. Question #920A 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?

- 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.

答案：B

解析：B – Configuring an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon SNS topic and configuring subscribers to receive events from the topic is a suitable solution for an event - driven, loosely coupled architecture using the pub / sub pattern. Amazon SNS is designed for this purpose and provides a cost - effective way to implement the publish / subscribe model. (A) using Amazon SQS is more suitable for a queue - based messaging system rather than a pub / sub pattern. (C) using Amazon Kinesis Data Streams with enhanced fan - out may be overkill for this scenario and may not be the most cost - effective option. (D) the type of API Gateway (HTTP or WebSocket) does not have a significant impact on meeting the requirements, and the key is the use of SNS for the pub / sub pattern.
解析：B – Configuring an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon SNS topic and configuring subscribers to receive events from the topic is a suitable

solution for an event - driven, loosely coupled architecture using the pub / sub pattern. Amazon SNS is designed for this purpose and provides a cost - effective way to implement the publish / subscribe model. (A) using Amazon SQS is more suitable for a queue - based messaging system rather than a pub / sub pattern. (C) using Amazon Kinesis Data Streams with enhanced fan - out may be overkill for this scenario and may not be the most cost - effective option. (D) the type of API Gateway (HTTP or WebSocket) does not have a significant impact on meeting the requirements, and the key is the use of SNS for the pub / sub pattern.

810. Question #921A 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?

- 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.

答案：A

解析: Based on the given scenario, the best solution to meet the company's requirements would be:

1. Resize the EC2 instance to an EC2 instance type that has more CPU capacity.
2. Configure an Auto Scaling group with a minimum and maximum size of 1.
3. Configure an RDS read replica for read requests.

This solution addresses the issues in the following ways:

1. Resizing the EC2 instance to a type with more CPU capacity will help reduce the high CPU utilization during peak usage times. This can be done by selecting an instance type from the same family with more vCPUs or moving to a more powerful instance family.
2. Configuring an Auto Scaling group, even with a minimum and maximum size of 1, provides several benefits:
 - It enables easier instance management and automatic recovery if the instance becomes unhealthy.
 - It allows for future scalability if the application is modified to support multiple instances.
 - It simplifies the process of changing instance types in the future if needed.
3. Adding an RDS read replica will significantly improve read request performance by:
 - Offloading read traffic from the primary database instance.
 - Allowing read requests to be distributed between the primary instance and the read replica.
 - Reducing the load on the primary database, which can improve overall application performance.

This solution maintains the current single-instance architecture while addressing the CPU utilization and database read performance issues. It also sets the groundwork for potential future scaling if the application is modified to support multiple instances. For implementation, I recommend referring to the official AWS documentation for detailed steps on resizing EC2 instances, setting up Auto Scaling groups, and configuring RDS read replicas. Always test these changes in a non-production environment before applying them to your production workload.

Sources

- [1] [Create an Auto Scaling group using parameters from an existing instance – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-from-instance.html>)
- [3] [Resize an EC2 instance – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-operations-for-vmware-admins/resize-instance.html>)
- [6] [Get more CPU or memory for your EC2 Linux instance | AWS re:Post]

(<https://repost.aws/knowledge-center/resize-instance>)

解析: Based on the given scenario, the best solution to meet the company's requirements would be:

1. Resize the EC2 instance to an EC2 instance type that has more CPU capacity.
2. Configure an Auto Scaling group with a minimum and maximum size of 1.
3. Configure an RDS read replica for read requests.

This solution addresses the issues in the following ways:

1. Resizing the EC2 instance to a type with more CPU capacity will help reduce the high CPU utilization during peak usage times. This can be done by selecting an instance type from the same family with more vCPUs or moving to a more powerful instance family.
2. Configuring an Auto Scaling group, even with a minimum and maximum size of 1, provides several benefits:
 - It enables easier instance management and automatic recovery if the instance becomes unhealthy.
 - It allows for future scalability if the application is modified to support multiple instances.
 - It simplifies the process of changing instance types in the future if needed.
3. Adding an RDS read replica will significantly improve read request performance by:
 - Offloading read traffic from the primary database instance.
 - Allowing read requests to be distributed between the primary instance and the read replica.
 - Reducing the load on the primary database, which can improve overall application performance.

This solution maintains the current single-instance architecture while addressing the CPU utilization and database read performance issues. It also sets the groundwork for potential future scaling if the application is modified to support multiple instances. For implementation, I recommend referring to the official AWS documentation for detailed steps on resizing EC2 instances, setting up Auto Scaling groups, and configuring RDS read replicas. Always test these changes in a non-production environment before applying them to your production workload.

Sources [1] [Create an Auto Scaling group using parameters from an existing instance – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-from-instance.html>) [3] [Resize an EC2 instance – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-operations-for-vmware-admins/resize-instance.html>) [6] [Get more CPU or memory for your

EC2 Linux instance | AWS re:Post]

(<https://repost.aws/knowledge-center/resize-instance>)

811. Question #922A 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?

- 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.

答案: B

解析: B – Defining IAM roles with fine-grained permissions based on the principle of least privilege and assigning each developer an IAM role ensures that developers have only the access they need to perform their tasks, minimizing the risk of unauthorized access to sensitive data. (A) sharing IAM user credentials is not a secure practice as it can lead to unauthorized access and is against best security practices. (C) creating IAM access keys and allowing developers to interact with AWS resources through API calls using the access keys can be a part of the access control solution, but it does not address the fine-grained permissions and least privilege principle as effectively as IAM roles. (D) creating an AWS Cognito user pool is typically used for user authentication and authorization in web and mobile applications, and may not be the most suitable solution for granting access to AWS resources for developers in this context.

解析: B – Defining IAM roles with fine-grained permissions based on the principle of least privilege and assigning each developer an IAM role ensures that developers have only the access they need to perform their tasks, minimizing the risk of unauthorized access to sensitive data. (A) sharing IAM user credentials is not a secure practice as it can lead to unauthorized access and is against best security practices. (C) creating IAM access keys and allowing developers to interact with AWS resources through API calls using the access keys can be a part of the access control solution, but it does not address the fine-grained permissions and least privilege principle as effectively as IAM roles. (D) creating an AWS Cognito user pool is typically used for user authentication and authorization in web and mobile applications, and may not be the most suitable solution for granting access to AWS resources for developers in this context.

812. Question #924A 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?

- 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.

答案: C

解析: C – AWS Identity and Access Management (IAM) Access Analyzer can be used to review all the company's resources and accounts, helping to identify which IAM users have more permissions than required. This tool is designed for analyzing access permissions and provides a straightforward way to assess the IAM configurations with the least

administrative overhead. (A) Network Access Analyzer is more focused on network access and may not be the most relevant tool for reviewing IAM permissions. (B) Creating a CloudWatch alarm for when an IAM user creates or modifies resources does not directly help in reviewing the existing permissions of all IAM users. (D) Amazon Inspector is used to find vulnerabilities in applications and infrastructure, not specifically in IAM policies.

解析: C – AWS Identity and Access Management (IAM) Access Analyzer can be used to review all the company's resources and accounts, helping to identify which IAM users have more permissions than required. This tool is designed for analyzing access permissions and provides a straightforward way to assess the IAM configurations with the least administrative overhead. (A) Network Access Analyzer is more focused on network access and may not be the most relevant tool for reviewing IAM permissions. (B) Creating a CloudWatch alarm for when an IAM user creates or modifies resources does not directly help in reviewing the existing permissions of all IAM users. (D) Amazon Inspector is used to find vulnerabilities in applications and infrastructure, not specifically in IAM policies.

813. Question #925A 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?

- 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.

答案: B

解析: B – Activating S3 Object Lock on the required objects and enabling compliance mode ensures that the sensitive documents are protected from deletion or modification for the fixed period of time specified in the policy. This meets the regulatory compliance requirements. (A) enabling governance mode may not be the appropriate mode for this specific requirement. (C) enabling versioning and setting a lifecycle policy to delete objects after a specified period does not provide the same level of protection as S3 Object Lock. (D) configuring an S3 Lifecycle policy to transition objects to S3 Glacier Flexible Retrieval for the retention duration does not prevent deletion or modification of the objects.

解析: B – Activating S3 Object Lock on the required objects and enabling compliance mode ensures that the sensitive documents are protected from deletion or modification for the fixed period of time specified in the policy. This meets the regulatory compliance requirements. (A) enabling governance mode may not be the appropriate mode for this specific requirement. (C) enabling versioning and setting a lifecycle policy to delete objects after a specified period does not provide the same level of protection as S3 Object Lock. (D) configuring an S3 Lifecycle policy to transition objects to S3 Glacier Flexible Retrieval for the retention duration does not prevent deletion or modification of the objects.

814. Question #926A 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?

- 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 rightscale the Fargate task.

答案: B

815. Question #927A 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?

- 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.**

答案: D

解析: D – Subscribing to AWS Shield Advanced provides a managed solution with proactive engagement to detect and mitigate DDoS attacks.

Configuring hosted zones in Route 53 and adding ALB resources as protected resources ensures that the application is protected. (A) AWS Config is primarily used for configuration management and may not be the best solution for detecting DDoS attacks. (B) AWS WAF can help protect against web application attacks, but it may not be sufficient for detecting and mitigating DDoS attacks. (C) Storing ALB access logs in an S3 bucket and using Amazon GuardDuty can detect some security issues, but it may not be specifically designed for DDoS attack detection and prevention.

解析: D – Subscribing to AWS Shield Advanced provides a managed solution with proactive engagement to detect and mitigate DDoS attacks.

Configuring hosted zones in Route 53 and adding ALB resources as protected resources ensures that the application is protected. (A) AWS Config is primarily used for configuration management and may not be the best solution for detecting DDoS attacks. (B) AWS WAF can help protect against web application attacks, but it may not be sufficient for detecting and mitigating DDoS attacks. (C) Storing ALB access logs in an S3 bucket and using Amazon GuardDuty can detect some security issues, but it may not be specifically designed for DDoS attack detection and prevention.

816. Question #928A 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?
- 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.

答案: B

解析: B – Recreating the NLB with a security group to allow only trusted IP addresses is a straightforward way to improve application security with minimal architectural change. By restricting access to the NLB based on trusted IP addresses, unauthorized attempts to access the application can be effectively filtered out. (A) implementing AWS WAF rules directly on the NLB may not be the most efficient solution as it may add complexity and may not provide the same level of control as using a security group. (C) deploying a second NLB in parallel with the existing NLB configured with a strict IP address allow list may not be necessary

and could add additional complexity and cost. (D) using AWS Shield Advanced is more focused on DDoS protection and may not address the specific issue of unauthorized access attempts based on IP addresses.

解析: B – Recreating the NLB with a security group to allow only trusted IP addresses is a straightforward way to improve application security with minimal architectural change. By restricting access to the NLB based on trusted IP addresses, unauthorized attempts to access the application can be effectively filtered out. (A) implementing AWS WAF rules directly on the NLB may not be the most efficient solution as it may add complexity and may not provide the same level of control as using a security group. (C) deploying a second NLB in parallel with the existing NLB configured with a strict IP address allow list may not be necessary and could add additional complexity and cost. (D) using AWS Shield Advanced is more focused on DDoS protection and may not address the specific issue of unauthorized access attempts based on IP addresses.

817. Question #930A 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?

- 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.

答案：A

解析：A – Running Amazon EC2 On-Demand Instances in an Auto Scaling group for the web portal ensures high availability. Using an AWS Lambda function to run the document extract program is a cost-effective and scalable solution that requires minimal implementation effort. Invoking the Lambda function when an employee uploads a new reimbursement document triggers the extraction process on-demand. (B) using EC2 Spot Instances for the web portal may not provide the same level of reliability as On-Demand Instances, and running the document extract program on Spot Instances may introduce additional complexity. (C) Purchasing a Savings Plan alone does not address the scalability and on-demand nature of the document extract program. (D) Creating an S3 bucket to host the web portal and using API Gateway and Lambda for existing functionalities may require more code changes and is not the least implementation effort option.

解析：A – Running Amazon EC2 On-Demand Instances in an Auto Scaling group for the web portal ensures high availability. Using an AWS Lambda function to run the document extract program is a cost-effective and scalable solution that requires minimal implementation effort. Invoking the Lambda function when an employee uploads a new reimbursement document triggers the extraction process on-demand. (B) using EC2 Spot Instances for the web portal may not provide the same level of reliability as On-Demand Instances, and running the document extract program on Spot Instances may introduce additional complexity. (C) Purchasing a Savings

Plan alone does not address the scalability and on-demand nature of the document extract program. (D) Creating an S3 bucket to host the web portal and using API Gateway and Lambda for existing functionalities may require more code changes and is not the least implementation effort option.

818. Question #932A 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?

- 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.

答案: C

解析: C – Using the Amazon VPC CNI plugin for Kubernetes and defining custom subnets in the VPC cluster for the pods to use allows the company to meet the requirement of using a custom subnet for pods in the VPC. It also ensures that the pods can communicate securely within the pods' VPC. (A) configuring AWS Transit Gateway is not directly related to managing custom subnet configurations for pods in Amazon EKS. (B) creating an AWS Direct Connect connection is for connecting the on-premises environment to AWS, but it does not address the specific requirement of using custom subnets for pods within the VPC. (D) implementing a Kubernetes network policy with pod anti-affinity rules is more about pod placement and does not directly address the issue of using custom subnets and ensuring secure communication within the VPC.

解析: C – Using the Amazon VPC CNI plugin for Kubernetes and defining custom subnets in the VPC cluster for the pods to use allows the company to meet the requirement of using a custom subnet for pods in the VPC. It also ensures that the pods can communicate securely within the pods' VPC. (A) configuring AWS Transit Gateway is not directly related to managing custom subnet configurations for pods in Amazon EKS. (B) creating an AWS Direct Connect connection is for connecting the on-premises environment to AWS, but it does not address the specific requirement of using custom subnets for pods within the VPC. (D) implementing a Kubernetes network policy with pod anti-affinity rules is more about pod placement and does not directly address the issue of using custom subnets and ensuring secure communication within the VPC.

819. Question #933A 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?**

- 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.

答案: A

解析: A – Modifying the RDS DB instance to use a Multi-AZ deployment is a straightforward and AWS-managed solution that mitigates the risk of a single point of failure with the least implementation effort. It can be

applied during the next maintenance window without the need for complex migration or manual restoration processes. (B) Migrating to Amazon DynamoDB and using AWS DMS for migration involves more complexity and may not be necessary for this specific requirement. (C) Creating a new RDS DB instance in a Multi - AZ deployment and manually restoring data from a snapshot is more time - consuming and may introduce additional risks. (D) Configuring the DB instance in an EC2 Auto Scaling group and using Route 53 for distribution is not the recommended approach for mitigating the risk of a single point of failure in an RDS database.

解析: A – Modifying the RDS DB instance to use a Multi – AZ deployment is a straightforward and AWS – managed solution that mitigates the risk of a single point of failure with the least implementation effort. It can be applied during the next maintenance window without the need for complex migration or manual restoration processes. (B) Migrating to Amazon DynamoDB and using AWS DMS for migration involves more complexity and may not be necessary for this specific requirement. (C) Creating a new RDS DB instance in a Multi – AZ deployment and manually restoring data from a snapshot is more time – consuming and may introduce additional risks. (D) Configuring the DB instance in an EC2 Auto Scaling group and using Route 53 for distribution is not the recommended approach for mitigating the risk of a single point of failure in an RDS database.

820. Question #934A 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?

- 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.

答案：A

解析：A – Amazon FSx for NetApp ONTAP provides a managed storage service that supports both NFS and SMB access. Configuring multi – protocol access allows the company to consolidate the file servers and share files between the protocols. It also offers redundancy at the Availability Zone level. (B) Creating two EC2 instances and using them for separate file server access does not provide the same level of managed service and redundancy as Amazon FSx for NetApp ONTAP. (C) Using separate FSx services for SMB and NFS access is not as efficient as using a single service with multi – protocol access. (D) Amazon S3 is an object storage service and may not be the best fit for file sharing requirements that require NFS and SMB access.

解析：A – Amazon FSx for NetApp ONTAP provides a managed storage service that supports both NFS and SMB access. Configuring multi – protocol access allows the company to consolidate the file servers and share files between the protocols. It also offers redundancy at the Availability Zone level. (B) Creating two EC2 instances and using them for separate file server access does not provide the same level of managed service and redundancy as Amazon FSx for NetApp ONTAP. (C) Using separate FSx services for SMB and NFS access is not as efficient as using a single service with multi – protocol access. (D) Amazon S3 is an object storage service and may not be the best fit for file sharing requirements that require NFS and SMB access.

821. Question #937A 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**?

- 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.

答案：C

解析：C – Configuring AWS Compute Optimizer for cost recommendations for the EC2 instances, the Auto Scaling group, and the EBS volumes provides a comprehensive and automated solution to identify cost optimizations. It offers real – time insights and recommendations based on the usage patterns and configurations of these resources, allowing the company to make informed decisions to optimize costs. (A) Creating an AWS Cost and Usage Report and searching it for cost recommendations is a manual and time – consuming process. (B) Creating Amazon CloudWatch billing alerts may provide some notifications, but it does not provide detailed cost recommendations and analysis. (D) Configuring AWS Compute Optimizer only for the EC2 instances and using a Cost and Usage Report for the Auto Scaling group and EBS volumes is not as efficient as using Compute Optimizer for all the resources.

解析：C – Configuring AWS Compute Optimizer for cost recommendations for the EC2 instances, the Auto Scaling group, and the EBS volumes provides a comprehensive and automated solution to identify cost optimizations. It offers real – time insights and recommendations based on the usage patterns and configurations of these resources, allowing the company to make informed decisions to optimize costs. (A) Creating an AWS Cost and Usage Report and searching it for cost recommendations is a manual and time – consuming process. (B) Creating Amazon CloudWatch billing alerts may provide some notifications, but it does not provide detailed cost

recommendations and analysis. (D) Configuring AWS Compute Optimizer only for the EC2 instances and using a Cost and Usage Report for the Auto Scaling group and EBS volumes is not as efficient as using Compute Optimizer for all the resources.

822. Question #938A 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?

- 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

答案: D

解析: D – Configuring an Amazon Elastic File System (Amazon EFS) file system and mounting it across all instances provides a high – performing solution for sharing data between EC2 instances within a VPC. Amazon EFS is designed for scalable file storage and can handle concurrent access from multiple instances, making it suitable for a media store application. (A) Creating an Amazon S3 bucket and calling the service APIs from each instance's application may introduce additional latency and is not the most efficient way to share data between instances. (B) Creating an Amazon S3 bucket and configuring all instances to access it as a mounted volume is not a typical use case for S3 and may not provide the performance and scalability required for a media store. (C) Configuring an Amazon EBS volume and mounting it across all instances is not a scalable solution as EBS volumes are limited to a single instance.

解析: D – Configuring an Amazon Elastic File System (Amazon EFS) file system and mounting it across all instances provides a high – performing

solution for sharing data between EC2 instances within a VPC. Amazon EFS is designed for scalable file storage and can handle concurrent access from multiple instances, making it suitable for a media store application. (A) Creating an Amazon S3 bucket and calling the service APIs from each instance's application may introduce additional latency and is not the most efficient way to share data between instances. (B) Creating an Amazon S3 bucket and configuring all instances to access it as a mounted volume is not a typical use case for S3 and may not provide the performance and scalability required for a media store. (C) Configuring an Amazon EBS volume and mounting it across all instances is not a scalable solution as EBS volumes are limited to a single instance.

823. Question #939A 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?

- 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

答案: B

解析: B – Since the read replica has a constant 25% CPU usage after the end - of - year activities, resizing it to a smaller instance size will optimize the cost without compromising the performance for future growth. There is no need to make changes to the primary instance as its CPU usage is still at 60%. (A) Deleting the read replica may not be the best

solution as it may be needed for future read – only queries. (C) Resizing the read replica to a larger instance size and resizing the primary instance to a smaller instance size may not be necessary as the primary instance's CPU usage indicates that it is still handling the workload adequately. (D) Deleting the read replica and resizing the primary instance to a larger size may not be the most cost – effective solution as the primary instance's CPU usage does not suggest a need for increased capacity.

解析: B – Since the read replica has a constant 25% CPU usage after the end – of – year activities, resizing it to a smaller instance size will optimize the cost without compromising the performance for future growth. There is no need to make changes to the primary instance as its CPU usage is still at 60%. (A) Deleting the read replica may not be the best solution as it may be needed for future read – only queries. (C) Resizing the read replica to a larger instance size and resizing the primary instance to a smaller instance size may not be necessary as the primary instance's CPU usage indicates that it is still handling the workload adequately. (D) Deleting the read replica and resizing the primary instance to a larger size may not be the most cost – effective solution as the primary instance's CPU usage does not suggest a need for increased capacity.

824. Question #940A 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?

- 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.

答案: D

解析: waiting...

解析: waiting...

825. Question #942A 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?

- 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**

答案: D

解析: D – Using server - side encryption with customer managed AWS KMS keys allows the company to have control over the encryption keys, enabling automatic rotation every year and tracking the key rotation using AWS CloudTrail. It also minimizes costs as the company manages the keys. (A) Using SSE - C requires the company to manage the keys themselves, which can be complex and may not be the best option for automatic rotation and tracking. (B) SSE - S3 uses Amazon S3 managed keys, but it may not provide the level of control and tracking required by the company's security policies. (C) SSE - KMS uses AWS KMS keys, but it may not be the most cost - effective option as it may incur additional costs compared to customer managed keys.

解析: D – Using server – side encryption with customer managed AWS KMS keys allows the company to have control over the encryption keys, enabling automatic rotation every year and tracking the key rotation using AWS CloudTrail. It also minimizes costs as the company manages the keys. (A) Using SSE – C requires the company to manage the keys themselves, which can be complex and may not be the best option for automatic rotation and tracking. (B) SSE – S3 uses Amazon S3 managed keys, but it may not provide the level of control and tracking required by the company's security policies. (C) SSE – KMS uses AWS KMS keys, but it may not be the most cost – effective option as it may incur additional costs compared to customer managed keys.

826. Question #943A 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?

- 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.

答案: C

解析: C – Tagging all the AWS resources with a key for cost and a value of the application's name and activating cost allocation tags allows the company to easily track and allocate costs to each application. Using Cost Explorer to get the desired information provides a cost – effective way to analyze the cost breakdown for the applications. (A) Using AWS Budgets to download data into a.csv file and looking up the information

may be time – consuming and may not provide the detailed breakdown needed. (B) Loading AWS Cost and Usage Reports into an Amazon RDS DB instance and running SQL queries can be complex and may incur additional costs. (D) **Using the AWS Billing and Cost Management console to download bills and look up the information may not be the most efficient way to get the detailed cost breakdown for each application.**

解析: C – Tagging all the AWS resources with a key for cost and a value of the application's name and activating cost allocation tags allows the company to easily track and allocate costs to each application. Using Cost Explorer to get the desired information provides a cost – effective way to analyze the cost breakdown for the applications. (A) Using AWS Budgets to download data into a.csv file and looking up the information may be time – consuming and may not provide the detailed breakdown needed. (B) Loading AWS Cost and Usage Reports into an Amazon RDS DB instance and running SQL queries can be complex and may incur additional costs. (D) **Using the AWS Billing and Cost Management console to download bills and look up the information may not be the most efficient way to get the detailed cost breakdown for each application.**

827. Question #944An 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?

- 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).

答案：B

解析：B – Deploying Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones ensures high availability and scalability for the web application. Deploying a Multi – AZ RDS DB instance provides redundancy for the database. Using Amazon CloudFront to distribute static assets improves performance and availability. (A) Deploying EC2 instances and the RDS DB instance in a single Availability Zone does not provide sufficient redundancy and resilience. (C) Serving static assets directly from the EC2 instances may not be the most efficient solution, and deploying the RDS DB instance in a second Availability Zone for cross – AZ redundancy alone may not be enough. (D) Using AWS Lambda functions and Amazon Aurora Serverless v2 may not be the best choice for a web application that requires continuous service, and storing static assets in Amazon EFS One Zone – IA may not provide the same level of performance and availability as using Amazon CloudFront.

解析：B – Deploying Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones ensures high availability and scalability for the web application. Deploying a Multi – AZ RDS DB instance provides redundancy for the database. Using Amazon CloudFront to distribute static assets improves performance and availability. (A) Deploying EC2 instances and the RDS DB instance in a single Availability Zone does not provide sufficient redundancy and resilience. (C) Serving static assets directly from the EC2 instances may not be the most efficient solution, and deploying the RDS DB instance in a second Availability Zone for cross – AZ redundancy alone may not be enough. (D) Using AWS Lambda functions and Amazon Aurora Serverless v2 may not be the best choice for a web application that requires continuous service, and storing static assets in Amazon EFS One Zone – IA may not provide the same level of performance and availability as using Amazon CloudFront.

828. Question #945 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?

- 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.

答案: C

解析: C – Deploying a Gateway Load Balancer (GWLB) in the networking account and configuring the application accounts to send traffic to the GWLB by using an interface GWLB endpoint ensures that the security appliance can inspect interactions between applications across AWS accounts. GWLB is designed for this purpose and provides a scalable and efficient solution. (A) Deploying an NLB and using an interface VPC endpoint may not be the most suitable option for this scenario. (B) Deploying an ALB in the application accounts to send traffic directly to the security appliance may not provide the centralized control and inspection required. (D) Deploying an interface VPC endpoint in the application accounts to send traffic directly to the security appliance may not provide the same level of scalability and management as using a GWLB.

解析: C – Deploying a Gateway Load Balancer (GWLB) in the networking account and configuring the application accounts to send traffic to the

GWLB by using an interface GWLB endpoint ensures that the security appliance can inspect interactions between applications across AWS accounts. GWLB is designed for this purpose and provides a scalable and efficient solution. (A) Deploying an NLB and using an interface VPC endpoint may not be the most suitable option for this scenario. (B) Deploying an ALB in the application accounts to send traffic directly to the security appliance may not provide the centralized control and inspection required. (D) Deploying an interface VPC endpoint in the application accounts to send traffic directly to the security appliance may not provide the same level of scalability and management as using a GWLB.

829. Question #946A 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?

- 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

答案：A

解析：waiting...

解析：waiting...

830. Question #947A 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?

- 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.

答案: B

解析: B – Storing the database credentials as a secret in AWS Secrets Manager and configuring it to automatically rotate the credentials every 30 days provides a secure and automated solution for managing the credentials. Updating the Lambda function to retrieve the credentials from the secret is a straightforward step. This approach minimizes the operational overhead compared to the other options. (A) Using AWS Systems Manager Parameter Store may not provide the same level of security and automatic rotation capabilities as AWS Secrets Manager. (C) Storing the credentials as an encrypted Lambda environment variable and writing a custom Lambda function to rotate the credentials requires more development and maintenance effort. (D) Using AWS KMS for key management may be overkill for this scenario and may add unnecessary complexity.

解析: B – Storing the database credentials as a secret in AWS Secrets Manager and configuring it to automatically rotate the credentials every 30 days provides a secure and automated solution for managing the credentials. Updating the Lambda function to retrieve the credentials from the secret is a straightforward step. This approach minimizes the

operational overhead compared to the other options. (A) Using AWS Systems Manager Parameter Store may not provide the same level of security and automatic rotation capabilities as AWS Secrets Manager. (C) Storing the credentials as an encrypted Lambda environment variable and writing a custom Lambda function to rotate the credentials requires more development and maintenance effort. (D) Using AWS KMS for key management may be overkill for this scenario and may add unnecessary complexity.

831. Question #948A 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?

- 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.

答案：A

解析：A – Configuring the AWS DMS replication instance with a Multi - AZ deployment allows for provisioning instances across multiple Availability Zones, ensuring high availability and the ability to handle varying amounts of data replication. This solution can allocate the required capacity based on the needs of the replication task. (B) Creating an AWS DMS Serverless replication task may not be the most suitable option as it might not provide the same level of control and customization as a Multi - AZ deployment. (C) Using Amazon EC2 Auto Scaling to scale the AWS DMS replication instance requires additional configuration and management,

and may not be as efficient as a dedicated DMS solution. (D) Provisioning AWS DMS replication capacity using Amazon ECS with an AWS Fargate launch type may introduce unnecessary complexity and may not be the most optimized solution for data replication from an on – premises Oracle database to Amazon RDS for Oracle.

解析：A – Configuring the AWS DMS replication instance with a Multi – AZ deployment allows for provisioning instances across multiple Availability Zones, ensuring high availability and the ability to handle varying amounts of data replication. This solution can allocate the required capacity based on the needs of the replication task. (B) Creating an AWS DMS Serverless replication task may not be the most suitable option as it might not provide the same level of control and customization as a Multi – AZ deployment. (C) Using Amazon EC2 Auto Scaling to scale the AWS DMS replication instance requires additional configuration and management, and may not be as efficient as a dedicated DMS solution. (D) Provisioning AWS DMS replication capacity using Amazon ECS with an AWS Fargate launch type may introduce unnecessary complexity and may not be the most optimized solution for data replication from an on – premises Oracle database to Amazon RDS for Oracle.

832. Question #949A 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?

- 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.

答案: D

解析: D – Using AWS PrivateLink to create a private connection between the application's VPC and the third – party SaaS provider provides secure and private connectivity while minimizing public internet exposure. AWS PrivateLink allows for direct connectivity between the VPC and the SaaS application over a private network, ensuring data privacy and security.

(A) Implementing an AWS Site – to – Site VPN may add complexity and may not be the most efficient solution for this specific requirement. (B) Deploying AWS Transit Gateway is typically used for managing traffic between multiple VPCs or on – premises networks and may not be necessary for connecting to a third – party SaaS provider. (C) Configuring AWS PrivateLink to allow only outbound traffic without enabling the third – party SaaS provider to establish a connection may not meet the requirements of a fully private and secure connection.

解析: D – Using AWS PrivateLink to create a private connection between the application's VPC and the third – party SaaS provider provides secure and private connectivity while minimizing public internet exposure. AWS PrivateLink allows for direct connectivity between the VPC and the SaaS application over a private network, ensuring data privacy and security.

(A) Implementing an AWS Site – to – Site VPN may add complexity and may not be the most efficient solution for this specific requirement. (B) Deploying AWS Transit Gateway is typically used for managing traffic between multiple VPCs or on – premises networks and may not be necessary for connecting to a third – party SaaS provider. (C) Configuring AWS PrivateLink to allow only outbound traffic without enabling the third – party SaaS provider to establish a connection may not meet the requirements of a fully private and secure connection.

833. Question #950A 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?

- 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.

答案: C

解析: Based on the requirements provided, the solution that best meets the needs for connecting the company's corporate network to its VPC while providing encryption and security controls is: Configure AWS Site-to-Site VPN to connect to the VPC, and implement security groups and network ACLs to control traffic. Here's a breakdown of why this solution is recommended:

- 1. Encryption:
 - AWS Site-to-Site VPN provides encryption at the network layer (IPsec).
 - For session layer encryption, you can implement TLS for application-level communication.
- 2. Security Controls:

- VPC security groups act as a virtual firewall for EC2 instances, controlling inbound and outbound traffic at the instance level.
- Network ACLs provide an additional layer of security at the subnet level, allowing you to control traffic in and out of one or more subnets.
- 3. Restricted Access:
 - By configuring security groups and network ACLs, you can precisely define which traffic is allowed between AWS and on-premises systems, adhering to the principle of least privilege.

Implementation steps:

- 1. Set up an AWS Site-to-Site VPN connection

between your on-premises network and your AWS VPC. 2. Configure route tables in your VPC to direct traffic to the VPN connection. 3. Implement security groups for your EC2 instances, allowing only necessary inbound and outbound traffic. 4. Configure network ACLs for your subnets to provide an additional layer of security. 5. Implement TLS for application-level communication to ensure encryption at the session layer. Remember to regularly review and update your security configurations to maintain a strong security posture. Always test your configuration in a non-production environment before implementing in production. For the most up-to-date information on implementing this solution and best practices for security, please refer to the official AWS documentation on VPN, VPC security, and encryption. Sources [1] [Infrastructure Security – Introduction to AWS Security] (<https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/infrastructure-security.html>) [3] [Infrastructure protection – Applying Security Practices to a Network Workload on AWS for Communications Service Providers] (<https://docs.aws.amazon.com/whitepapers/latest/applying-security-practices-to-network-workload-for-csp/infrastructure-protection.html>) [6] [Security – Connected Mobility Solution on AWS] (<https://docs.aws.amazon.com/solutions/latest/connected-mobility-solution-on-aws/security-1.html>)

解析: Based on the requirements provided, the solution that best meets the needs for connecting the company's corporate network to its VPC while providing encryption and security controls is: Configure AWS Site-to-Site VPN to connect to the VPC, and implement security groups and network ACLs to control traffic. Here's a breakdown of why this solution is recommended:

1. **Encryption:**
 - AWS Site-to-Site VPN provides encryption at the network layer (IPsec).
 - For session layer encryption, you can implement TLS for application-level communication.
2. **Security Controls:**
 - VPC security groups act as a virtual firewall for EC2 instances, controlling inbound and outbound traffic at the instance level.
 - Network ACLs provide an additional layer of security at the subnet level, allowing you to control traffic in and out of one or more subnets.
3. **Restricted Access:**
 - By configuring security groups and network ACLs,

you can precisely define which traffic is allowed between AWS and on-premises systems, adhering to the principle of least privilege. Implementation steps: 1. Set up an AWS Site-to-Site VPN connection between your on-premises network and your AWS VPC. 2. Configure route tables in your VPC to direct traffic to the VPN connection. 3. Implement security groups for your EC2 instances, allowing only necessary inbound and outbound traffic. 4. Configure network ACLs for your subnets to provide an additional layer of security. 5. Implement TLS for application-level communication to ensure encryption at the session layer. Remember to regularly review and update your security configurations to maintain a strong security posture. Always test your configuration in a non-production environment before implementing in production. For the most up-to-date information on implementing this solution and best practices for security, please refer to the official AWS documentation on VPN, VPC security, and encryption. Sources [1] [Infrastructure Security – Introduction to AWS Security] (<https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/infrastructure-security.html>) [3] [Infrastructure protection – Applying Security Practices to a Network Workload on AWS for Communications Service Providers] (<https://docs.aws.amazon.com/whitepapers/latest/applying-security-practices-to-network-workload-for-csp/infrastructure-protection.html>) [6] [Security – Connected Mobility Solution on AWS] (<https://docs.aws.amazon.com/solutions/latest/connected-mobility-solution-on-aws/security-1.html>)

834. Question #951A 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?

- 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.

答案：C

解析：C – Storing the credentials in AWS Secrets Manager provides a secure and centralized location for managing secrets. Configuring the application to load the credentials from Secrets Manager simplifies the process and reduces the risk of exposing the credentials within the application. Setting up a credentials rotation schedule using an AWS Lambda function for Secrets Manager ensures that the credentials are regularly updated and enhances security. (A) Storing credentials in AWS KMS may not be the most suitable solution for this specific use case, as it is primarily used for key management rather than secret storage. (B) Storing credentials in encrypted local storage introduces the risk of credential leakage and requires manual management of the rotation schedule. (D) AWS Systems Manager Parameter Store is more commonly used for storing configuration parameters rather than sensitive credentials.

解析：C – Storing the credentials in AWS Secrets Manager provides a secure and centralized location for managing secrets. Configuring the application to load the credentials from Secrets Manager simplifies the process and reduces the risk of exposing the credentials within the application. Setting up a credentials rotation schedule using an AWS Lambda function for Secrets Manager ensures that the credentials are regularly updated and enhances security. (A) Storing credentials in AWS KMS may not be the most suitable solution for this specific use case, as it is primarily used for key management rather than secret storage. (B)

Storing credentials in encrypted local storage introduces the risk of credential leakage and requires manual management of the rotation schedule. (D) AWS Systems Manager Parameter Store is more commonly used for storing configuration parameters rather than sensitive credentials.

835. Question #952A 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?

- 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.

答案：A

解析：A – Creating a new S3 bucket with server – side encryption using AWS KMS multi – Region keys (SSE – KMS) ensures encryption at rest and replication to a different AWS Region. Configuring Cross – Region Replication (CRR) and loading the data into the new bucket simplifies the process. Using Amazon Athena to query the data provides a serverless and scalable solution for analyzing the data with SQL, minimizing operational overhead. (B) Using Amazon RDS for querying the data may not be the most serverless and cost – effective option. (C) Configuring CRR on the existing bucket may introduce complexities and may not be the cleanest

approach. (D) Using Amazon RDS for querying the data and using AWS KMS multi – Region keys may not be the most efficient combination for this requirement.

解析: A – Creating a new S3 bucket with server – side encryption using AWS KMS multi – Region keys (SSE – KMS) ensures encryption at rest and replication to a different AWS Region. Configuring Cross – Region Replication (CRR) and loading the data into the new bucket simplifies the process. Using Amazon Athena to query the data provides a serverless and scalable solution for analyzing the data with SQL, minimizing operational overhead. (B) Using Amazon RDS for querying the data may not be the most serverless and cost – effective option. (C) Configuring CRR on the existing bucket may introduce complexities and may not be the cleanest approach. (D) Using Amazon RDS for querying the data and using AWS KMS multi – Region keys may not be the most efficient combination for this requirement.

836. Question #953A 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?

- 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.

答案：A

解析：A – Moving uploaded images to Amazon S3 Glacier Deep Archive is a cost – effective option for long – term storage of infrequently accessed images. Moving premium user – generated AI images to S3 Standard ensures quick access for premium users. Moving non – premium user – generated AI images to S3 Standard – Infrequent Access (S3 Standard – IA) is suitable for less frequently accessed images. This solution balances cost and access requirements. (B) Moving all generated AI images to S3 Glacier Flexible Retrieval may not be necessary for premium user images that require more frequent access. (C) Using Amazon S3 One Zone – Infrequent Access (S3 One Zone – IA) may not provide the same level of durability and availability as S3 Glacier Deep Archive for long – term storage. (D) Moving all generated AI images to S3 Glacier Flexible Retrieval may not be the most cost – effective option for non – premium user images that are accessed less frequently.

解析：A – Moving uploaded images to Amazon S3 Glacier Deep Archive is a cost – effective option for long – term storage of infrequently accessed images. Moving premium user – generated AI images to S3 Standard ensures quick access for premium users. Moving non – premium user – generated AI images to S3 Standard – Infrequent Access (S3 Standard – IA) is suitable for less frequently accessed images. This solution balances cost and access requirements. (B) Moving all generated AI images to S3 Glacier Flexible Retrieval may not be necessary for premium user images that require more frequent access. (C) Using Amazon S3 One Zone – Infrequent Access (S3 One Zone – IA) may not provide the same level of durability and availability as S3 Glacier Deep Archive for long – term storage. (D) Moving all generated AI images to S3 Glacier Flexible Retrieval may not be the most cost – effective option for non – premium user images that are accessed less frequently.

837. Question #954A 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?

- 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.

答案: D

解析: D – Directing the requests from the API into an Amazon SQS queue allows for decoupling of the API and the ML models. Deploying the ML models as Amazon ECS services that read from the queue provides a scalable and flexible solution. Using auto scaling for Amazon ECS to scale both the cluster capacity and number of services based on the size of the SQS queue ensures that the resources are allocated based on the actual demand, handling the irregular usage patterns effectively. (A)

Deploying the ML models as AWS Lambda functions may not be suitable for handling batches of requests and may have limitations in terms of memory and processing power. (B) Using an ALB to invoke the ML models may not be the most efficient way to handle the asynchronous nature of the requests and the irregular usage patterns. (C) Increasing the number of vCPUs for the Lambda functions based on the size of the SQS queue may not be the most effective scaling strategy, as the ML models may require more resources than just vCPUs.

解析: D – Directing the requests from the API into an Amazon SQS queue allows for decoupling of the API and the ML models. Deploying the ML models as Amazon ECS services that read from the queue provides a scalable and flexible solution. Using auto scaling for Amazon ECS to scale both the cluster capacity and number of services based on the size of the SQS queue ensures that the resources are allocated based on the actual demand, handling the irregular usage patterns effectively. (A) Deploying the ML models as AWS Lambda functions may not be suitable for handling batches of requests and may have limitations in terms of memory and processing power. (B) Using an ALB to invoke the ML models may not be the most efficient way to handle the asynchronous nature of the requests and the irregular usage patterns. (C) Increasing the number of vCPUs for the Lambda functions based on the size of the SQS queue may not be the most effective scaling strategy, as the ML models may require more resources than just vCPUs.

838. Question #955A 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?
- 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.

答案：A

解析：A – Deploying the DR infrastructure in a second AWS Region with an ALB and an Auto Scaling group, setting the desired and maximum capacity of the Auto Scaling group to a minimum value, converting the Aurora MySQL DB cluster to an Aurora global database, and configuring Amazon Route 53 for an active – passive failover with ALB endpoints meets the requirements. The active – passive failover ensures that the DR solution is only used when the primary infrastructure is unavailable, and the conversion to an Aurora global database provides the necessary data replication and recovery capabilities within the 30 – minute recovery time target. (B) Configuring active – active failover may not be the best approach as it may introduce complexity and may not be necessary when the DR solution does not need to support customer usage when the primary infrastructure is healthy. (C) Backing up the data and restoring it in a new Aurora MySQL DB cluster in the second Region can be time – consuming and may not meet the 30 – minute recovery time requirement. (D) Backing up the infrastructure configuration and creating the required infrastructure in a second Region may not be the most efficient solution,

and setting the Auto Scaling group desired capacity to zero may not be appropriate as it would require scaling up the instances during a failover, which could take time.

解析: A – Deploying the DR infrastructure in a second AWS Region with an ALB and an Auto Scaling group, setting the desired and maximum capacity of the Auto Scaling group to a minimum value, converting the Aurora MySQL DB cluster to an Aurora global database, and configuring Amazon Route 53 for an active – passive failover with ALB endpoints meets the requirements. The active – passive failover ensures that the DR solution is only used when the primary infrastructure is unavailable, and the conversion to an Aurora global database provides the necessary data replication and recovery capabilities within the 30 – minute recovery time target. (B) Configuring active – active failover may not be the best approach as it may introduce complexity and may not be necessary when the DR solution does not need to support customer usage when the primary infrastructure is healthy. (C) Backing up the data and restoring it in a new Aurora MySQL DB cluster in the second Region can be time – consuming and may not meet the 30 – minute recovery time requirement. (D) Backing up the infrastructure configuration and creating the required infrastructure in a second Region may not be the most efficient solution, and setting the Auto Scaling group desired capacity to zero may not be appropriate as it would require scaling up the instances during a failover, which could take time.

839. Question #956A 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?

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.

答案：D

解析：To meet the company's requirements for migrating their data processing application to AWS while keeping costs low, I recommend the following solution:

1. Use Amazon EC2 instances to run the short-lived batch jobs. Choose instance types optimized for batch processing workloads.
2. Implement Amazon EC2 Auto Scaling to automatically adjust the number of instances based on the workload, ensuring cost-efficiency.
3. Store the generated data in Amazon S3 using the following tiered approach:
 - a. Initially, store data in S3 Standard for the first 30 days of frequent access.
 - b. After 30 days, use S3 Lifecycle policies to automatically transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) for the remainder of the 2-year retention period.
4. Set up an S3 Lifecycle rule to automatically delete the data after the 2-year retention period to avoid unnecessary storage costs.
5. Use Amazon CloudWatch to monitor the application's performance and costs, allowing for further optimization.
6. Consider using AWS Batch for managing and scaling the batch computing jobs if the workload becomes more complex over time.

This solution addresses the requirements by:

- Ensuring the batch jobs can run without disruption on EC2 instances.
- Providing cost-effective storage for the generated data, with S3 Standard for frequent access and S3 Standard-IA for long-term retention.
- Automating data lifecycle management to minimize storage costs.
- Allowing for

scalability and cost optimization through Auto Scaling and monitoring.

Sources [1] [Choosing an AWS storage service – Choosing an AWS storage service] (<https://docs.aws.amazon.com/decision-guides/latest/storage-on-a-ws-how-to-choose/choosing-aws-storage-service.html>) [3] [Community | Optimizing Network Traffic and Cost in AWS During Migration] (<https://community.aws/content/2fdHdKYvkBVCx7Y2VymX0FpKtpg/optimizing-network-traffic-and-cost-in-aws-during-migration>) [6] [Storage Solutions for .NET Applications on AWS – Developing and Deploying .NET Applications on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/storage-solutions-for-.net-applications-on-aws.html>)

解析: To meet the company's requirements for migrating their data processing application to AWS while keeping costs low, I recommend the following solution:

1. Use Amazon EC2 instances to run the short-lived batch jobs. Choose instance types optimized for batch processing workloads.
2. Implement Amazon EC2 Auto Scaling to automatically adjust the number of instances based on the workload, ensuring cost-efficiency.
3. Store the generated data in Amazon S3 using the following tiered approach:
 - a. Initially, store data in S3 Standard for the first 30 days of frequent access.
 - b. After 30 days, use S3 Lifecycle policies to automatically transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) for the remainder of the 2-year retention period.
4. Set up an S3 Lifecycle rule to automatically delete the data after the 2-year retention period to avoid unnecessary storage costs.
5. Use Amazon CloudWatch to monitor the application's performance and costs, allowing for further optimization.
6. Consider using AWS Batch for managing and scaling the batch computing jobs if the workload becomes more complex over time.

This solution addresses the requirements by:

- Ensuring the batch jobs can run without disruption on EC2 instances.
- Providing cost-effective storage for the generated data, with S3 Standard for frequent access and S3 Standard-IA for long-term retention.
- Automating data lifecycle management to minimize storage costs.
- Allowing for scalability and cost optimization through Auto Scaling and monitoring.

Sources [1] [Choosing an AWS storage service – Choosing an AWS storage service] (<https://docs.aws.amazon.com/decision-guides/latest/storage-on-a-ws-how-to-choose/choosing-aws-storage-service.html>)

[ws-how-to-choose/choosing-aws-storage-service.html](https://aws.amazon.com/community/ws-how-to-choose/choosing-aws-storage-service.html)) [3] [Community | Optimizing Network Traffic and Cost in AWS During Migration] (<https://community.aws/content/2fdHdKYvkBVCx7Y2VymX0FpKtpg/optimizing-network-traffic-and-cost-in-aws-during-migration>) [6] [Storage Solutions for .NET Applications on AWS – Developing and Deploying .NET Applications on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/develop-deploy-dotnet-apps-on-aws/storage-solutions-for-.net-applications-on-aws.html>)

840. Question #958A 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?

- 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.

答案：A

解析：A – Creating an Amazon RDS Proxy and assigning it to the DB instance can help reduce failover time by providing a layer of abstraction and caching, improving the performance and availability of the database. The RDS Proxy can handle the connection pooling and routing, reducing the impact of failovers on the application. (B) Creating a read replica and moving the read traffic to it may not directly address the issue of reducing failover time for the primary DB instance. (C) Enabling Performance Insights to monitor the CPU load can help identify the timeouts, but it does not directly solve the problem of reducing failover time. (D) Taking regular automatic snapshots and copying them to multiple AWS Regions is a backup and disaster recovery strategy, but it does not address the issue of reducing failover time

during database failovers.

解析: A – Creating an Amazon RDS Proxy and assigning it to the DB instance can help reduce failover time by providing a layer of abstraction and caching, improving the performance and availability of the database. The RDS Proxy can handle the connection pooling and routing, reducing the impact of failovers on the application. (B) Creating a read replica and moving the read traffic to it may not directly address the issue of reducing failover time for the primary DB instance. (C) Enabling Performance Insights to monitor the CPU load can help identify the timeouts, but it does not directly solve the problem of reducing failover time. (D) Taking regular automatic snapshots and copying them to multiple AWS Regions is a backup and disaster recovery strategy, but it does not address the issue of reducing failover time during database failovers.

841. Question #959A 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?

- 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.

答案: D

解析: D – Creating an Amazon EventBridge rule that invokes AWS Lambda functions to start and stop the RDS instances based on a schedule is a straightforward and efficient solution with the least operational

overhead. EventBridge can easily integrate with the RDS instances and trigger the Lambda functions at the specified times. (A) Creating a CloudWatch alarm and a Lambda function requires additional configuration and may not be the most straightforward approach. (B) Using AWS Trusted Advisor report and a Lambda function is not directly related to scheduling the start and stop of the RDS instances. (C) Creating AWS Systems Manager State Manager associations may be more complex and may not be the most suitable option for this specific requirement.

解析: D – Creating an Amazon EventBridge rule that invokes AWS Lambda functions to start and stop the RDS instances based on a schedule is a straightforward and efficient solution with the least operational overhead. EventBridge can easily integrate with the RDS instances and trigger the Lambda functions at the specified times. (A) Creating a CloudWatch alarm and a Lambda function requires additional configuration and may not be the most straightforward approach. (B) Using AWS Trusted Advisor report and a Lambda function is not directly related to scheduling the start and stop of the RDS instances. (C) Creating AWS Systems Manager State Manager associations may be more complex and may not be the most suitable option for this specific requirement.

842. Question #960A 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?

- 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.

答案：B

解析：B – Configuring S3 Cross – Region Replication (CRR) from the company's S3 bucket to one of the marketing firm's S3 buckets in the new geographic region allows the data to be replicated closer to the marketing firm, minimizing data transfer costs when they request the data. This solution ensures that the data is available locally in the target region, reducing the need for long – distance data transfers. (A) Configuring the Requester Pays feature may not directly address the issue of minimizing data transfer costs, as it only shifts the cost responsibility to the requester. (C) Configuring AWS Resource Access Manager to share the S3 bucket does not necessarily minimize the data transfer costs, as the data still needs to be transferred over the network. (D) Configuring the company's S3 bucket to use S3 Intelligent – Tiering and syncing it to the marketing firm's S3 bucket may not be the most effective solution for minimizing data transfer costs, as it does not address the issue of replicating the data to a closer location.

解析：B – Configuring S3 Cross – Region Replication (CRR) from the company's S3 bucket to one of the marketing firm's S3 buckets in the new geographic region allows the data to be replicated closer to the marketing firm, minimizing data transfer costs when they request the data. This solution ensures that the data is available locally in the target region, reducing the need for long – distance data transfers. (A) Configuring the Requester Pays feature may not directly address the issue of minimizing data transfer costs, as it only shifts the cost responsibility to the requester. (C) Configuring AWS Resource Access Manager to share the S3 bucket does not necessarily minimize the data transfer costs, as the data still needs to be transferred over the network. (D) Configuring the company's S3 bucket to use S3 Intelligent – Tiering and syncing it to the marketing firm's S3 bucket may not be the most effective solution for minimizing data transfer costs, as it does not address the issue of replicating the data to a closer location.

843. Question #961A 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?

- 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.

答案：A

解析：A – Configuring an AWS WAF web ACL for the Global Accelerator accelerator to block traffic by using rate – based rules is a straightforward and effective solution to mitigate DDoS attacks with the least implementation effort. By setting up rate – based rules in the WAF web ACL, the accelerator can block excessive traffic and protect the website. (B) Configuring an AWS Lambda function to read ALB metrics and update a VPC network ACL is more complex and may not be the most efficient solution for mitigating DDoS attacks. (C) Configuring an AWS WAF web ACL on the ALB may not be as effective as configuring it on the Global Accelerator accelerator, as the attack traffic may already reach the ALB before being blocked. (D) Configuring an Amazon CloudFront distribution in front of the Global Accelerator accelerator may introduce additional complexity and may not be necessary for mitigating DDoS attacks in this case.

解析：A – Configuring an AWS WAF web ACL for the Global Accelerator accelerator to block traffic by using rate – based rules is a straightforward and effective solution to mitigate DDoS attacks with the

least implementation effort. By setting up rate – based rules in the WAF web ACL, the accelerator can block excessive traffic and protect the website. (B) Configuring an AWS Lambda function to read ALB metrics and update a VPC network ACL is more complex and may not be the most efficient solution for mitigating DDoS attacks. (C) Configuring an AWS WAF web ACL on the ALB may not be as effective as configuring it on the Global Accelerator accelerator, as the attack traffic may already reach the ALB before being blocked. (D) Configuring an Amazon CloudFront distribution in front of the Global Accelerator accelerator may introduce additional complexity and may not be necessary for mitigating DDoS attacks in this case.

844. Question #962A 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?

- 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.

答案: A

解析: A – Using an Amazon Athena SQL query with the Amazon Athena DynamoDB connector is a serverless and cost – effective solution to calculate performance metrics on a recurring schedule. It has minimal impact on the table's provisioned read and write capacity as it does not require loading the data into another system. (B) Using an AWS Glue job

with the AWS Glue DynamoDB export connector may introduce additional overhead and complexity. (C) Using an Amazon Redshift COPY command requires loading the data into Redshift, which may not be the most efficient option for this use case. (D) Using an Amazon EMR job with an Apache Hive external table is more suitable for big data processing and may be overkill for calculating performance metrics on a daily basis.

解析: A – Using an Amazon Athena SQL query with the Amazon Athena DynamoDB connector is a serverless and cost – effective solution to calculate performance metrics on a recurring schedule. It has minimal impact on the table's provisioned read and write capacity as it does not require loading the data into another system. (B) Using an AWS Glue job with the AWS Glue DynamoDB export connector may introduce additional overhead and complexity. (C) Using an Amazon Redshift COPY command requires loading the data into Redshift, which may not be the most efficient option for this use case. (D) Using an Amazon EMR job with an Apache Hive external table is more suitable for big data processing and may be overkill for calculating performance metrics on a daily basis.

845. Question #963A 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?

- 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.

答案：C

解析：C – Creating an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed allows for decoupling and asynchronous processing. The Auto Scaling group can be configured to add and remove EC2 instances based on the number of items in the SQS queue, ensuring that the processing capacity scales according to the workload. This solution meets the requirements of running in parallel, adding and removing instances as needed, and durably storing the job items. (A) Using an Amazon SNS topic may not be the best choice for holding and managing the jobs as it is more suitable for notification purposes. (B) Scaling based on network usage may not accurately reflect the workload and the need for processing jobs. (D) Using an SNS topic and scaling based on the number of messages published may not be as efficient as using an SQS queue for job management.

解析：C – Creating an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed allows for decoupling and asynchronous processing. The Auto Scaling group can be configured to add and remove EC2 instances based on the number of items in the SQS queue, ensuring that the processing capacity scales according to the workload. This solution meets the requirements of running in parallel, adding and removing instances as needed, and durably storing the job items. (A) Using an Amazon SNS topic may not be the best choice for holding and managing the jobs as it is more suitable for notification purposes. (B) Scaling based on network usage may not accurately reflect the workload and the need for processing jobs. (D) Using an SNS topic and scaling based on the number of messages published may not be as efficient as

using an SQS queue for job management.

846. Question #964A 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?

- 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.

答案: D

解析: D – Using Amazon Elastic Container Service (Amazon ECS) with AWS Fargate to deploy a containerized application provides a scalable and serverless solution for running the application. Amazon RDS with a Multi - AZ deployment offers high availability and durability for storing the product data. Storing the product images in an Amazon S3 bucket is a cost - effective and scalable storage solution. This combination meets the requirements with the least operational overhead compared to the other options. (A) Using an Amazon EC2 instance in an Auto Scaling group and an

Application Load Balancer requires more management and may not be as scalable as using Fargate. Storing product images in an Amazon RDS DB instance may not be the most efficient storage option for images. (B) Using AWS Lambda functions to manage the existing monolithic application may not be the best approach for a large volume of product data and may introduce more complexity. (C) Using Amazon EKS with an Amazon EC2 deployment and AWS Step Functions may be overkill for this scenario and may increase operational overhead. Storing product images in Amazon S3 Glacier Deep Archive may not be necessary for immediate access to the images.

解析: D – Using Amazon Elastic Container Service (Amazon ECS) with AWS Fargate to deploy a containerized application provides a scalable and serverless solution for running the application. Amazon RDS with a Multi – AZ deployment offers high availability and durability for storing the product data. Storing the product images in an Amazon S3 bucket is a cost – effective and scalable storage solution. This combination meets the requirements with the least operational overhead compared to the other options. (A) Using an Amazon EC2 instance in an Auto Scaling group and an Application Load Balancer requires more management and may not be as scalable as using Fargate. Storing product images in an Amazon RDS DB instance may not be the most efficient storage option for images. (B) Using AWS Lambda functions to manage the existing monolithic application may not be the best approach for a large volume of product data and may introduce more complexity. (C) Using Amazon EKS with an Amazon EC2 deployment and AWS Step Functions may be overkill for this scenario and may increase operational overhead. Storing product images in Amazon S3 Glacier Deep Archive may not be necessary for immediate access to the images.

847. Question #965A 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?

- 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.

答案：A

解析：waiting...

解析：waiting...

848. Question #966A 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?

- 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.

答案：B

解析：B – Creating EMR runtime roles and configuring the cluster to use them allows for fine – grained access control to AWS services. Each team can be assigned a specific runtime role with the necessary permissions, ensuring that the big data workloads can only access the services they need. Using the runtime roles to submit the workloads enforces this

access control. (A) Configuring interface VPC endpoints for each AWS service may not provide the same level of access control and may be more complex to manage. (C) Creating an EC2 IAM instance profile may not be the best approach as it does not provide the same level of isolation and control as runtime roles. (D) Creating an EMR security configuration with the EnableApplicationScopedIAMRole option set to false may not be sufficient to restrict access to IMDSv2 and may not provide the necessary access control to AWS services.

解析: B – Creating EMR runtime roles and configuring the cluster to use them allows for fine – grained access control to AWS services. Each team can be assigned a specific runtime role with the necessary permissions, ensuring that the big data workloads can only access the services they need. Using the runtime roles to submit the workloads enforces this access control. (A) Configuring interface VPC endpoints for each AWS service may not provide the same level of access control and may be more complex to manage. (C) Creating an EC2 IAM instance profile may not be the best approach as it does not provide the same level of isolation and control as runtime roles. (D) Creating an EMR security configuration with the EnableApplicationScopedIAMRole option set to false may not be sufficient to restrict access to IMDSv2 and may not provide the necessary access control to AWS services.

849. Question #967A 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?

- 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.

答案：A

解析：A – Using an Amazon SQS FIFO queue ensures that the form data is processed in the order it is submitted and that each form is processed exactly once. This meets the requirements of processing submitted forms quickly and ensuring no data is lost. (B) An Amazon API Gateway HTTP API is not designed for storing and forwarding form data in this context. (C) An Amazon SQS standard queue does not guarantee the order of processing or that each form will be processed exactly once. (D) An AWS Step Functions workflow may be more complex than necessary for this simple form processing requirement.

解析：A – Using an Amazon SQS FIFO queue ensures that the form data is processed in the order it is submitted and that each form is processed exactly once. This meets the requirements of processing submitted forms quickly and ensuring no data is lost. (B) An Amazon API Gateway HTTP API is not designed for storing and forwarding form data in this context. (C) An Amazon SQS standard queue does not guarantee the order of processing or that each form will be processed exactly once. (D) An AWS Step Functions workflow may be more complex than necessary for this simple form processing requirement.

850. Question #968A 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?
- 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.

答案：D

解析：D – Amazon Kinesis Data Streams is designed for ingesting and processing streaming data. Amazon OpenSearch Service is a suitable choice for searching and indexing the data. Amazon QuickSight can be used for creating visualizations. This combination of services provides an AWS native solution that meets the requirements of the finance company. (A) Using Amazon EC2 instances, Amazon S3, Amazon Athena, and Amazon Managed Grafana may not provide the same level of real-time processing and search capabilities as the Kinesis Data Streams and OpenSearch Service combination. (B) Amazon EMR and Amazon Redshift may be more suitable for batch processing and data warehousing, rather than real-time streaming data processing. (C) Amazon EKS and Amazon DynamoDB may not be the best fit for this specific use case, and Amazon CloudWatch is primarily used for monitoring rather than data search and visualization.

解析：D – Amazon Kinesis Data Streams is designed for ingesting and processing streaming data. Amazon OpenSearch Service is a suitable choice for searching and indexing the data. Amazon QuickSight can be used for creating visualizations. This combination of services provides an AWS native solution that meets the requirements of the finance company. (A) Using Amazon EC2 instances, Amazon S3, Amazon Athena, and Amazon Managed Grafana may not provide the same level of real-time processing and search capabilities as the Kinesis Data Streams and OpenSearch Service combination. (B) Amazon EMR and Amazon Redshift may be more suitable for batch processing and data warehousing, rather than real-time streaming

data processing. (C) Amazon EKS and Amazon DynamoDB may not be the best fit for this specific use case, and Amazon CloudWatch is primarily used for monitoring rather than data search and visualization.

851. Question #969A 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?

- 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.

答案: A

解析: A – Using AWS App2Container to containerize the application and deploying it to Amazon ECS on AWS Fargate using an AWS CloudFormation template provides a serverless and scalable solution. AWS Fargate eliminates the need to manage the underlying infrastructure, reducing operational overhead. (B) Deploying to Amazon ECS on Amazon EC2 instances requires more management of the EC2 instances, increasing operational complexity. (C) AWS App Runner is designed for simpler applications and may not be the best choice for a resource-intensive application that requires specific containerization and deployment configurations. (D)

Deploying to Amazon EKS on Amazon EC2 instances also involves more complex management and may not be the most efficient option for reducing operational overhead.

解析: A – Using AWS AppContainer to containerize the application and deploying it to Amazon ECS on AWS Fargate using an AWS CloudFormation template provides a serverless and scalable solution. AWS Fargate eliminates the need to manage the underlying infrastructure, reducing operational overhead. (B) Deploying to Amazon ECS on Amazon EC2 instances requires more management of the EC2 instances, increasing operational complexity. (C) AWS App Runner is designed for simpler applications and may not be the best choice for a resource-intensive application that requires specific containerization and deployment configurations. (D) Deploying to Amazon EKS on Amazon EC2 instances also involves more complex management and may not be the most efficient option for reducing operational overhead.

852. Question #970A 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?

- 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.

答案: D

解析: D – AWS Secrets Manager is designed to securely store and manage secrets, such as usernames and passwords. Using AWS CloudFormation and the BatchGetSecretValue API to retrieve the credentials from Secrets Manager simplifies the process and reduces operational overhead. (A) AWS Systems Manager Parameter Store is more suitable for storing configuration parameters rather than sensitive credentials. (B) Using AWS Batch may not be necessary for retrieving credentials and can add complexity. (C) Similar to option A, using AWS Systems Manager Parameter Store for storing employee credentials is not the best choice due to its intended use for configuration data.

解析: D – AWS Secrets Manager is designed to securely store and manage secrets, such as usernames and passwords. Using AWS CloudFormation and the BatchGetSecretValue API to retrieve the credentials from Secrets Manager simplifies the process and reduces operational overhead. (A) AWS Systems Manager Parameter Store is more suitable for storing configuration parameters rather than sensitive credentials. (B) Using AWS Batch may not be necessary for retrieving credentials and can add complexity. (C) Similar to option A, using AWS Systems Manager Parameter Store for storing employee credentials is not the best choice due to its intended use for configuration data.

853. Question #971A 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?

- 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.

答案：D

解析：D – Creating an Amazon S3 bucket in the ap – northeast – 1 Region and setting up an Amazon CloudFront distribution with the S3 bucket as the origin allows for faster content delivery. Downloading the software by using signed URLs provides secure access. This solution minimizes the deployment latency with the least operational overhead. (A) Setting up an Amazon CloudFront distribution with a CachingDisabled cache policy may not be the most efficient way to reduce latency. (B) Creating a second S3 bucket in the us – east – 1 Region and configuring replication adds complexity and may not be necessary. (C) Configuring Amazon S3 Transfer Acceleration can improve transfer speeds, but it may not be as straightforward as using CloudFront.

解析：D – Creating an Amazon S3 bucket in the ap – northeast – 1 Region and setting up an Amazon CloudFront distribution with the S3 bucket as the origin allows for faster content delivery. Downloading the software by using signed URLs provides secure access. This solution minimizes the deployment latency with the least operational overhead. (A) Setting up an Amazon CloudFront distribution with a CachingDisabled cache policy may not be the most efficient way to reduce latency. (B) Creating a second S3 bucket in the us – east – 1 Region and configuring replication adds complexity and may not be necessary. (C) Configuring Amazon S3 Transfer Acceleration can improve transfer speeds, but it may not be as straightforward as using CloudFront.

854. Question #972A 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?

- 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 from one EBS volume in one Availability Zone to another EBS volume in the second Availability Zone.
- 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 Internet Small Computer Systems Interface (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 as storage attached to the EC2 instances. Set up Amazon EBS level replication to sync data from one io2 volume in one Availability Zone to another io2 volume in the second Availability Zone.

答案: A

解析: A – Configuring a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances and using Amazon FSx for Windows File Server as shared storage provides a highly available solution with low - latency access to block storage. Amazon FSx for Windows File Server is designed to meet the requirements of Windows

applications and provides seamless integration with the cluster. This solution requires less implementation effort compared to the other options. (B) Setting up application – level replication to sync data between EBS volumes can be complex and may not provide the same level of performance and reliability as using a dedicated file system like Amazon FSx. (C) Using Amazon FSx for NetApp ONTAP Multi – AZ file system with iSCSI protocol may introduce additional complexity and may not be the most straightforward solution. (D) Setting up Amazon EBS level replication can be challenging and may not be as efficient as using a dedicated file system for shared storage.

解析: A – Configuring a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances and using Amazon FSx for Windows File Server as shared storage provides a highly available solution with low – latency access to block storage. Amazon FSx for Windows File Server is designed to meet the requirements of Windows applications and provides seamless integration with the cluster. This solution requires less implementation effort compared to the other options. (B) Setting up application – level replication to sync data between EBS volumes can be complex and may not provide the same level of performance and reliability as using a dedicated file system like Amazon FSx. (C) Using Amazon FSx for NetApp ONTAP Multi – AZ file system with iSCSI protocol may introduce additional complexity and may not be the most straightforward solution. (D) Setting up Amazon EBS level replication can be challenging and may not be as efficient as using a dedicated file system for shared storage.

855. Question #975A 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?

- 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.

答案：A

解析：A – Configuring Amazon Athena to read the encrypted files and run SQL queries directly in Amazon S3 is a cost – effective solution for occasional SQL queries on the data. Athena is a serverless analytics service that can easily handle the processing of Parquet files stored in S3. It eliminates the need for managing and maintaining a separate data warehouse or processing cluster. (B) Amazon S3 Select may not be the most suitable option for running complex SQL queries or taking sample moving averages. (C) Configuring Amazon Redshift and using Redshift Spectrum and Redshift query editor v2 may involve more setup and cost compared to Athena for occasional queries. (D) Configuring Amazon EMR Serverless and using Apache SparkSQL can be more complex and resource – intensive than using Athena for this specific requirement.

解析：A – Configuring Amazon Athena to read the encrypted files and run SQL queries directly in Amazon S3 is a cost – effective solution for occasional SQL queries on the data. Athena is a serverless analytics service that can easily handle the processing of Parquet files stored in S3. It eliminates the need for managing and maintaining a separate data warehouse or processing cluster. (B) Amazon S3 Select may not be the most suitable option for running complex SQL queries or taking sample moving averages. (C) Configuring Amazon Redshift and using Redshift Spectrum and Redshift query editor v2 may involve more setup and cost compared to Athena for occasional queries. (D) Configuring Amazon EMR Serverless and using Apache SparkSQL can be more complex and resource – intensive than

using Athena for this specific requirement.

856. Question #976A 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?

- 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.

答案：B

解析：B – Implementing an Amazon Route 53 geoproximity routing policy allows for routing traffic based on the user's location, ensuring that they are directed to the EC2 instances that are closest to them. Using an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region helps in efficiently handling the traffic and ensuring high availability. (A) While an Amazon Route 53 geolocation routing policy can route traffic based on the user's location, using an Application Load Balancer may not be the most suitable choice for this scenario. (C) An Amazon Route 53 multivalue answer routing policy is not specifically designed for routing traffic based on the user's location. (D) An Amazon Route 53 weighted routing policy is typically used for distributing traffic based on predefined weights

rather than the user's location.

解析: B – Implementing an Amazon Route 53 geoproximity routing policy allows for routing traffic based on the user's location, ensuring that they are directed to the EC2 instances that are closest to them. Using an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region helps in efficiently handling the traffic and ensuring high availability. (A) While an Amazon Route 53 geolocation routing policy can route traffic based on the user's location, using an Application Load Balancer may not be the most suitable choice for this scenario. (C) An Amazon Route 53 multivalue answer routing policy is not specifically designed for routing traffic based on the user's location. (D) An Amazon Route 53 weighted routing policy is typically used for distributing traffic based on predefined weights rather than the user's location.

857. Question #977A 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?

- 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.

答案: A

解析: A – Configuring encryption at rest for Amazon RDS for MySQL using AWS KMS managed keys is a straightforward and AWS-managed solution. Configuring AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit also simplifies the process and ensures secure communication. This combination provides the necessary encryption with the least operational overhead. (B) Configuring IPsec tunnels for encryption in transit can be more complex and may require additional configuration and management. (C) Implementing third-party application-level data encryption adds complexity and may not be necessary when AWS-provided solutions can meet the requirements. (D) Configuring a VPN connection for encryption in transit may not be the most efficient or straightforward approach compared to using ACM SSL/TLS certificates.

解析: A – Configuring encryption at rest for Amazon RDS for MySQL using AWS KMS managed keys is a straightforward and AWS-managed solution. Configuring AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit also simplifies the process and ensures secure communication. This combination provides the necessary encryption with the least operational overhead. (B) Configuring IPsec tunnels for encryption in transit can be more complex and may require additional configuration and management. (C) Implementing third-party application-level data encryption adds complexity and may not be necessary when AWS-provided solutions can meet the requirements. (D) Configuring a VPN connection for encryption in transit may not be the most efficient or straightforward approach compared to using ACM SSL/TLS certificates.

858. Question #978A 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?

- 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.

答案：A

解析：A – Creating Amazon RDS automated backups and setting the retention period to 90 days is a simple and automated solution that meets the requirements with the least operational overhead. RDS automated backups handle the backup and retention process automatically, ensuring that the data is retained for the required 90 days and can be restored to a specific point in time within the 14-day window. (B) Creating an Amazon RDS manual snapshot every day and deleting manual snapshots older than 90 days is a manual and time-consuming process that introduces more operational overhead. (C) Using the Amazon Aurora Clone feature for Oracle may not be applicable as the database is being migrated to Amazon RDS for Oracle, not Amazon Aurora. (D) Creating a backup plan using AWS Backup for Amazon RDS may add additional complexity and may not be the most straightforward solution for this specific requirement.

解析：A – Creating Amazon RDS automated backups and setting the retention period to 90 days is a simple and automated solution that meets the requirements with the least operational overhead. RDS automated backups handle the backup and retention process automatically, ensuring that the data is retained for the required 90 days and can be restored to a specific point in time within the 14-day window. (B) Creating an Amazon RDS manual snapshot every day and deleting manual snapshots older than 90 days is a manual and time-consuming process that introduces more operational overhead. (C) Using the Amazon Aurora Clone feature for Oracle may not be applicable as the database is being migrated to Amazon RDS for Oracle, not Amazon Aurora. (D) Creating a backup plan using AWS Backup for Amazon RDS may add additional complexity and may not be the

most straightforward solution for this specific requirement.

859. Question #979A 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?

- 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.

答案: B

解析: B – Deploying the database on Amazon Aurora Serverless allows for automatic scaling of the database capacity based on actual usage. This is particularly suitable for an application with variable database usage and a read-heavy workload. Aurora Serverless can dynamically adjust the resources allocated to the database, ensuring cost optimization while providing the necessary performance. (A) Using Provisioned IOPS SSD storage on Amazon RDS may not be the most cost-effective option as it requires pre-provisioning storage and IOPS, which may not be fully utilized in a variable workload. (C) Amazon DynamoDB is a NoSQL database and may not be the best fit for a relational database requirement. (D) Using magnetic storage and read replicas on Amazon RDS may not provide the same level of automatic scaling and cost optimization as Aurora Serverless.

解析: B – Deploying the database on Amazon Aurora Serverless allows for automatic scaling of the database capacity based on actual usage. This is

particularly suitable for an application with variable database usage and a read-heavy workload. Aurora Serverless can dynamically adjust the resources allocated to the database, ensuring cost optimization while providing the necessary performance. (A) Using Provisioned IOPS SSD storage on Amazon RDS may not be the most cost-effective option as it requires pre-provisioning storage and IOPS, which may not be fully utilized in a variable workload. (C) Amazon DynamoDB is a NoSQL database and may not be the best fit for a relational database requirement. (D) Using magnetic storage and read replicas on Amazon RDS may not provide the same level of automatic scaling and cost optimization as Aurora Serverless.

860. Question #980A 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?

- 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:

答案：A

解析：A – Creating a gateway endpoint for Amazon S3 attached to the VPC allows for direct and secure access to the S3 buckets within the VPC.

Updating the IAM instance profile policy to provide access only to the specific buckets that the application needs ensures fine-grained access control. This solution provides the necessary security with the least operational overhead. (B) Creating a NAT gateway and using a security group to allow access to only Amazon S3 adds complexity and may not be the most efficient solution. (C) While creating a gateway endpoint and updating the IAM instance profile policy with a Deny action and condition key can provide access control, it may not be the simplest approach. (D) Creating a NAT Gateway and assigning bucket policies with a Deny action and condition key is more complex and may not be the most straightforward solution.

解析: A – Creating a gateway endpoint for Amazon S3 attached to the VPC allows for direct and secure access to the S3 buckets within the VPC. Updating the IAM instance profile policy to provide access only to the specific buckets that the application needs ensures fine-grained access control. This solution provides the necessary security with the least operational overhead. (B) Creating a NAT gateway and using a security group to allow access to only Amazon S3 adds complexity and may not be the most efficient solution. (C) While creating a gateway endpoint and updating the IAM instance profile policy with a Deny action and condition key can provide access control, it may not be the simplest approach. (D) Creating a NAT Gateway and assigning bucket policies with a Deny action and condition key is more complex and may not be the most straightforward solution.

861. Question #981A 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?

- 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.

答案: B

解析: B – Enabling IAM Identity Center with an Identity Center directory and creating and configuring permission sets with granular access to Amazon RDS and Amazon S3 allows for centralized management of user credentials and access permissions. Assigning all the teams to groups with specific access using the permission sets simplifies the process of granting and managing access based on team responsibilities. This solution complies with the principle of least privilege and has the least operational overhead compared to the other options. (A) Using IAM roles with customized IAM policies can be effective, but managing individual roles for each team may be more complex. (C) Creating individual IAM users and assigning IAM roles based on user needs can be time-consuming and may not be the most efficient approach. (D) Using AWS Organizations to create separate accounts for each team and implementing cross-account IAM roles adds additional complexity and may not be necessary for this scenario.

解析: B – Enabling IAM Identity Center with an Identity Center directory and creating and configuring permission sets with granular access to Amazon RDS and Amazon S3 allows for centralized management of user credentials and access permissions. Assigning all the teams to groups with specific access using the permission sets simplifies the process of granting and managing access based on team responsibilities. This solution complies with the principle of least privilege and has the least operational overhead compared to the other options. (A) Using IAM roles with customized IAM policies can be effective, but managing individual roles for each team may be more complex. (C) Creating individual IAM users and assigning IAM roles based on user needs can be time-consuming and may not be the most efficient approach. (D) Using AWS Organizations to create separate accounts for each team and implementing cross-account IAM roles adds additional complexity and may not be necessary for this scenario.

862. Question #982 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?

- 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.

答案：B

解析：Option B is the correct choice because it utilizes IAM Roles Anywhere, which allows applications running outside of AWS to securely obtain AWS credentials that grant access to AWS resources, such as an S3 bucket. By configuring the virtual machines to assume the role using the AWS CLI, the application can access the S3 bucket without exposing long-term credentials.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the correct choice because it utilizes IAM Roles Anywhere, which allows applications running outside of AWS to securely obtain AWS credentials that grant access to AWS resources, such as an S3 bucket. By configuring the virtual machines to assume the role using the AWS CLI, the application can access the S3 bucket without exposing long-term credentials.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

863. Question #983 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?

- 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 VPRoute 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.

答案：D

解析：Option D is the correct choice as it provides a centralized solution for multiple AWS accounts to access the on-premises network

services through AWS Transit Gateway. This approach reduces the operational overhead compared to creating individual DX connections (Option A), VPN connections (Option C), or managing VPC endpoints (Option B) for each

account. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the correct choice as it provides a centralized solution for multiple AWS accounts to access the on-premises network services through AWS Transit Gateway. This approach reduces the operational overhead compared to creating individual DX connections (Option A), VPN connections (Option C), or managing VPC endpoints (Option B) for each

account. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

864. Question #984 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.

- 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.

答案: A

解析: Option A is the correct choice because Amazon CloudFront is a cost-effective solution for distributing dynamic content globally. By configuring the existing ALB as the origin, the web application can serve content from the edge locations closest to the customers, improving the performance and reducing the load on the origin servers.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option A is the correct choice because Amazon CloudFront is a cost-effective solution for distributing dynamic content globally. By configuring the existing ALB as the origin, the web application can serve content from the edge locations closest to the customers, improving the performance and reducing the load on the origin servers.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

865. Question #985 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?

- 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)

答案：B

解析：Option B is the correct choice for a storage solution that offers both high durability and availability while being cost-effective. Amazon S3 Intelligent-Tiering automatically moves data to the most cost-effective access tier without performance impact or additional fees, making it suitable for data with varying access

patterns. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the correct choice for a storage solution that offers both high durability and availability while being cost-effective. Amazon S3 Intelligent-Tiering automatically moves data to the most cost-effective access tier without performance impact or additional fees, making it suitable for data with varying access

patterns. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

866. Question #986 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 SS0 (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?

- 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

答案: D

解析: Option D is the correct choice because Amazon EFS provides a highly available and resilient file system that can be accessed by multiple EC2 instances without significant changes to the application code. EFS scales easily and integrates well with Auto Scaling groups, making it ideal for applications that require shared storage.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the correct choice because Amazon EFS provides a highly available and resilient file system that can be accessed by multiple EC2 instances without significant changes to the application code. EFS scales easily and integrates well with Auto Scaling groups, making it ideal for applications that require shared storage.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

867. Question #989 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?

- 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.

答案：C

解析：Option C is the most cost-effective solution as it allows the company to maintain both automated and manual RDS backups while ensuring that only backups less than 30 days old are retained. This approach avoids the need to disable automated backups or manually delete backups, which could lead to data loss or increased operational overhead.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option C is the most cost-effective solution as it allows the company to maintain both automated and manual RDS backups while ensuring that only backups less than 30 days old are retained. This approach avoids the need to disable automated backups or manually delete backups, which could lead to data loss or increased operational overhead.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

868. Question #990 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?

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

答案: C

解析: Option C is the correct choice for a storage solution that supports NFS and can be used by the legacy application after migration to AWS.

Amazon EFS is designed to work with applications that require a shared file system and can be easily integrated with existing NFS-based workflows. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option C is the correct choice for a storage solution that supports NFS and can be used by the legacy application after migration to AWS.

Amazon EFS is designed to work with applications that require a shared file system and can be easily integrated with existing NFS-based workflows. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

869. Question #991 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?

- 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.

答案：C

解析：Option C is the correct choice for handling unexpected volumes of data with minimal operational overhead. By using Amazon SQS, the incoming data can be queued and processed asynchronously, allowing the application to scale and manage the load more effectively without losing data.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option C is the correct choice for handling unexpected volumes of data with minimal operational overhead. By using Amazon SQS, the incoming data can be queued and processed asynchronously, allowing the application to scale and manage the load more effectively without losing data.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

870. Question #992 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?

- 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.

答案：B

解析：Option B is the most secure solution for providing connectivity to the RDS cluster from an on-premises desktop client. By creating a VPC with private subnets and using AWS Site-to-Site VPN, the traffic between the on-premises network and the AWS environment is encrypted and secure.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the most secure solution for providing connectivity to the RDS cluster from an on-premises desktop client. By creating a VPC with private subnets and using AWS Site-to-Site VPN, the traffic between the on-premises network and the AWS environment is encrypted and secure.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

871. Question #993 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?

- 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.

答案：C

解析：Option C is the correct choice for reducing data transfer costs. By placing all EC2 instances in the same Availability Zone, data transfer between instances occurs within the same zone without incurring additional costs, which is more cost-effective than transferring data across different zones or regions.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option C is the correct choice for reducing data transfer costs. By placing all EC2 instances in the same Availability Zone, data transfer between instances occurs within the same zone without incurring

additional costs, which is more cost-effective than transferring data across different zones or regions.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

872. Question #994 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?

- 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.

答案：A

解析: Option A is the least operationally intensive solution for managing database credentials. Using AWS Secrets Manager to rotate credentials every 14 days automates the process and ensures that the credentials are encrypted and securely managed, reducing the need for manual intervention.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option A is the least operationally intensive solution for managing database credentials. Using AWS Secrets Manager to rotate credentials every 14 days automates the process and ensures that the credentials are encrypted and securely managed, reducing the need for manual intervention.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

873. Question #995 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?

- A. Use AWS Lambda functions to process videos. Store video metadata in Amazon DynamoDB. Store video content in Amazon S3 IntelligentTiering.
- 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 and to decouple processing tasks.
- 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.

答案: C

解析: Option C is the correct choice for a scalable and cost-effective solution for video processing. Using EC2 instances with an Auto Scaling group allows the application to handle varying loads, while storing video content in Amazon S3 Standard and using SQS for task queuing ensures efficient processing and cost control.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option C is the correct choice for a scalable and cost-effective solution for video processing. Using EC2 instances with an Auto Scaling group allows the application to handle varying loads, while storing video content in Amazon S3 Standard and using SQS for task queuing ensures efficient processing and cost control.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

874. Question #996 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?

- 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.

答案: C

解析: Option C is the solution with the least operational overhead for migrating an on-premises Kubernetes application to AWS. AWS Fargate eliminates the need to manage the underlying compute infrastructure,

allowing the company to focus on deploying and managing the application without worrying about server maintenance.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option C is the solution with the least operational overhead for migrating an on-premises Kubernetes application to AWS. AWS Fargate eliminates the need to manage the underlying compute infrastructure, allowing the company to focus on deploying and managing the application without worrying about server maintenance.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

875. Question #997 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?

- 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.

答案：C

解析：Option C is the most cost-effective solution for a scalable and backed-up database. Amazon Aurora Serverless automatically scales with application traffic and provides automated backups to Amazon S3, reducing the need for manual management and optimization of resources.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option C is the most cost-effective solution for a scalable and backed-up database. Amazon Aurora Serverless automatically scales with

application traffic and provides automated backups to Amazon S3, reducing the need for manual management and optimization of resources.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

876. Question #998 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?

- 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.

答案：A

解析：Option A is the correct solution to ensure that traffic to Amazon S3 does not use the public endpoint. By creating a gateway VPC endpoint, the traffic is routed through the private network, ensuring secure and private access to the S3 bucket.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option A is the correct solution to ensure that traffic to Amazon S3 does not use the public endpoint. By creating a gateway VPC endpoint, the traffic is routed through the private network, ensuring secure and

private access to the S3 bucket.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

877. Question #999 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?

- 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.

答案：B

解析：Option B is the recommended solution to improve the performance of the website during product catalog searches. Implementing Amazon ElastiCache for Redis to cache the product catalog data reduces the load on the MySQL database, improving response times and overall website performance. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the recommended solution to improve the performance of the website during product catalog searches. Implementing Amazon ElastiCache for Redis to cache the product catalog data reduces the load on the MySQL database, improving response times and overall website performance. 答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

878. Question #1000 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?

- 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.

答案：B

解析：Option B is the most operationally efficient solution because it uses an AWS Storage Gateway Volume Gateway with cached volumes as iSCSI targets. This setup allows for low-latency access to frequently accessed data while storing the data in Amazon S3. The cached volumes keep a local copy of the data for fast retrieval, which is ideal for on-premises applications that require quick access to storage.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the most operationally efficient solution because it uses an AWS Storage Gateway Volume Gateway with cached volumes as iSCSI targets. This setup allows for low-latency access to frequently accessed data while storing the data in Amazon S3. The cached volumes keep a local copy of the data for fast retrieval, which is ideal for on-premises applications that require quick access to storage.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

879. Question #1001A company operates a food delivery service. Because of recent growth, the company's order processing system is experiencing

scaling problems during peak traffic hours. The current architecture includes Amazon EC2 instances in an Auto Scaling group that collect orders from an application. A second group of EC2 instances in an Auto Scaling group fulfills the 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 adequately during peak traffic hours. Which solution will meet these requirements?

- A. Use Amazon CloudWatch to monitor the CPUUtilization metric for each instance in both Auto Scaling groups. Configure each Auto Scaling group's minimum capacity to meet its peak workload value.
- B. Use Amazon CloudWatch to monitor the CPUUtilization metric for each instance in both Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic to create additional Auto Scaling groups on demand.
- C. Provision two Amazon Simple Queue Service (Amazon SQS) queues. Use one SQS queue for order collection. Use the second SQS queue for order fulfillment. Configure the EC2 instances to poll their respective queues. Scale the Auto Scaling groups based on notifications that the queues send.
- D. Provision two Amazon Simple Queue Service (Amazon SQS) queues. Use one SQS queue for order collection. Use the second SQS queue for order fulfillment. Configure the EC2 instances to poll their respective queues. Scale the Auto Scaling groups based on the number of messages in each queue.

答案: D

解析: Option D is the solution that will meet the requirements by ensuring that both the order collection and fulfillment processes can scale adequately during peak traffic hours. By provisioning two Amazon SQS queues and configuring the EC2 instances to poll their respective queues, the system can handle increased load. Scaling the Auto Scaling groups based on the number of messages in each queue allows for dynamic adjustment to the workload, preventing data loss and ensuring efficient

processing.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the solution that will meet the requirements by ensuring that both the order collection and fulfillment processes can scale adequately during peak traffic hours. By provisioning two Amazon SQS queues and configuring the EC2 instances to poll their respective queues, the system can handle increased load. Scaling the Auto Scaling groups based on the number of messages in each queue allows for dynamic adjustment to the workload, preventing data loss and ensuring efficient processing.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

880. Question #1002 An online gaming company is transitioning user data storage to Amazon DynamoDB to support the company's growing user base. The current architecture includes DynamoDB tables that contain user profiles, achievements, and in-game transactions. The company needs to design a robust, continuously available, and resilient DynamoDB architecture to maintain a seamless gaming experience for users. Which solution will meet these requirements MOST cost-effectively?

- A. Create DynamoDB tables in a single AWS Region. Use on-demand capacity mode. Use global tables to replicate data across multiple Regions.
- B. Use DynamoDB Accelerator (DAX) to cache frequently accessed data. Deploy tables in a single AWS Region and enable auto scaling. Configure Cross-Region Replication manually to additional Regions.
- C. Create DynamoDB tables in multiple AWS Regions. Use on-demand capacity mode. Use DynamoDB Streams for Cross-Region Replication between Regions.
- D. Use DynamoDB global tables for automatic multi-Region replication. Deploy tables in multiple AWS Regions. Use provisioned capacity mode. Enable auto scaling.

答案: D

解析: Option D is the most cost-effective solution for a robust, continuously available, and resilient DynamoDB architecture. Using DynamoDB global tables for automatic multi-Region replication ensures high availability and data redundancy. Deploying tables in multiple AWS

Regions with provisioned capacity mode and enabling auto scaling allows the system to handle varying loads without manual intervention, providing a seamless gaming experience for users.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the most cost-effective solution for a robust, continuously available, and resilient DynamoDB architecture. Using DynamoDB global tables for automatic multi-Region replication ensures high availability and data redundancy. Deploying tables in multiple AWS Regions with provisioned capacity mode and enabling auto scaling allows the system to handle varying loads without manual intervention, providing a seamless gaming experience for users.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

881. Question #1003 A company runs its media rendering application on premises. The company wants to reduce storage costs and has moved all data to Amazon S3. The on-premises rendering application needs low-latency access to storage. The company needs to design a storage solution for the application. The storage solution must maintain the desired application performance. Which storage solution will meet these requirements in the MOST cost-effective way?

- A. Use Mountpoint for Amazon S3 to access the data in Amazon S3 for the on-premises application.
- B. Configure an Amazon S3 File Gateway to provide storage for the on-premises application.
- C. Copy the data from Amazon S3 to Amazon FSx for Windows File Server. Configure an Amazon FSx File Gateway to provide storage for the on-premises application.
- D. Configure an on-premises file server. Use the Amazon S3 API to connect to S3 storage. Configure the application to access the storage from the on-premises file server.

答案: B

解析: Option B is the most cost-effective storage solution that meets the requirement for low-latency access to storage for the on-premises rendering application. Configuring an Amazon S3 File Gateway provides a

seamless integration with the existing S3 storage, allowing the application to access data with low latency while leveraging the scalability and cost-effectiveness of Amazon S3.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option B is the most cost-effective storage solution that meets the requirement for low-latency access to storage for the on-premises rendering application. Configuring an Amazon S3 File Gateway provides a seamless integration with the existing S3 storage, allowing the application to access data with low latency while leveraging the scalability and cost-effectiveness of Amazon S3.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

882. Question #1004A company hosts its enterprise resource planning (ERP) system in the us-east-1 Region. The system runs on Amazon EC2 instances. Customers use a public API that is hosted on the EC2 instances to exchange information with the ERP system. International customers report slow API response times from their data centers. Which solution will improve response times for the international customers MOST cost-effectively?

- A. Create an AWS Direct Connect connection that has a public virtual interface (VIF) to provide connectivity from each customer's data center to us-east-1. Route customer API requests by using a Direct Connect gateway to the ERP system API.
- B. Set up an Amazon CloudFront distribution in front of the API. Configure the CachingOptimized managed cache policy to provide improved cache efficiency.
- C. Set up AWS Global Accelerator. Configure listeners for the necessary ports. Configure endpoint groups for the appropriate Regions to distribute traffic. Create an endpoint in the group for the API.
- D. Use AWS Site-to-Site VPN to establish dedicated VPN tunnels between Regions and customer networks. Route traffic to the API over the VPN connections.

答案: B

解析: Based on the scenario described, the most cost-effective solution to improve response times for international customers accessing the ERP system's API is: B. Set up an Amazon CloudFront distribution in front of the API. Configure the CachingOptimized managed cache policy to provide improved cache efficiency. Here's why this is the best solution:

1. **Global reach:** CloudFront is a content delivery network (CDN) with a global network of edge locations. This allows it to cache and serve content closer to international customers, significantly reducing latency.
2. **Cost-effectiveness:** CloudFront is generally more cost-effective than setting up dedicated connections or using Global Accelerator for this use case. You pay only for the data transfer and requests you actually use.
3. **Caching benefits:** The CachingOptimized policy can help reduce the load on your origin servers (EC2 instances) by serving cached responses for repeated requests. This can improve performance and reduce costs associated with compute resources.
4. **Easy implementation:** Setting up a CloudFront distribution is relatively straightforward and doesn't require changes to your existing infrastructure.
5. **Scalability:** CloudFront can handle traffic spikes without additional configuration, providing a scalable solution for your growing international customer base.

Compared to the other options:

- Option A (Direct Connect) is more expensive and complex to set up, especially for multiple international locations. It's typically used for consistent, private network connections rather than improving public API access.
- Option C (Global Accelerator) can improve network performance but doesn't offer the caching benefits of CloudFront. It's often more suitable for non-HTTP/HTTPS traffic or when you need static IP addresses.

When implementing this solution, consider the following best practices:

1. Configure appropriate cache behaviors based on your API's characteristics.
2. Use HTTPS for secure communication between clients, CloudFront, and your origin.
3. Implement proper origin request policies to control which headers, cookies, and query strings are forwarded to your origin.
4. Monitor CloudFront metrics to optimize performance and cost over time.
5. Consider implementing AWS WAF with CloudFront for additional security at the edge.

Sources [1] [Optimize performance of

REST APIs – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/developerguide/rest-api-optimize.html>)

解析: Based on the scenario described, the most cost-effective solution to improve response times for international customers accessing the ERP system's API is: B. Set up an Amazon CloudFront distribution in front of the API. Configure the CachingOptimized managed cache policy to provide improved cache efficiency. Here's why this is the best solution:

1. **Global reach:** CloudFront is a content delivery network (CDN) with a global network of edge locations. This allows it to cache and serve content closer to international customers, significantly reducing latency.
2. **Cost-effectiveness:** CloudFront is generally more cost-effective than setting up dedicated connections or using Global Accelerator for this use case. You pay only for the data transfer and requests you actually use.
3. **Caching benefits:** The CachingOptimized policy can help reduce the load on your origin servers (EC2 instances) by serving cached responses for repeated requests. This can improve performance and reduce costs associated with compute resources.
4. **Easy implementation:** Setting up a CloudFront distribution is relatively straightforward and doesn't require changes to your existing infrastructure.
5. **Scalability:** CloudFront can handle traffic spikes without additional configuration, providing a scalable solution for your growing international customer base.

Compared to the other options:

- Option A (Direct Connect) is more expensive and complex to set up, especially for multiple international locations. It's typically used for consistent, private network connections rather than improving public API access.
- Option C (Global Accelerator) can improve network performance but doesn't offer the caching benefits of CloudFront. It's often more suitable for non-HTTP/HTTPS traffic or when you need static IP addresses.

When implementing this solution, consider the following best practices:

1. Configure appropriate cache behaviors based on your API's characteristics.
2. Use HTTPS for secure communication between clients, CloudFront, and your origin.
3. Implement proper origin request policies to control which headers, cookies, and query strings are forwarded to your origin.
4. Monitor CloudFront metrics to optimize performance and

cost over time. 5. Consider implementing AWS WAF with CloudFront for additional security at the edge. Sources [1] [Optimize performance of REST APIs – Amazon API Gateway] (<https://docs.aws.amazon.com/apigateway/latest/developerguide/rest-api-optimize.html>)

883. Question #1005 A company tracks customer satisfaction by using surveys that the company hosts on its website. The surveys sometimes reach thousands of customers every hour. Survey results are currently sent in email messages to the company so company employees can manually review results and assess customer sentiment. The company wants to automate the customer survey process. Survey results must be available for the previous 12 months. Which solution will meet these requirements in the MOST scalable way?

- A. Send the survey results data to an Amazon API Gateway endpoint that is connected to an Amazon Simple Queue Service (Amazon SQS) queue. Create an AWS Lambda function to poll the SQS queue, call Amazon Comprehend for sentiment analysis, and save the results to an Amazon DynamoDB table. Set the TTL for all records to 365 days in the future.
- B. Send the survey results data to an API that is running on an Amazon EC2 instance. Configure the API to store the survey results as a new record in an Amazon DynamoDB table, call Amazon Comprehend for sentiment analysis, and save the results in a second DynamoDB table. Set the TTL for all records to 365 days in the future.
- C. Write the survey results data to an Amazon S3 bucket. Use S3 Event Notifications to invoke an AWS Lambda function to read the data and call Amazon Rekognition for sentiment analysis. Store the sentiment analysis results in a second S3 bucket. Use S3 lifecycle policies on each bucket to expire objects after 365 days.
- D. Send the survey results data to an Amazon API Gateway endpoint that is connected to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the SQS queue to invoke an AWS Lambda function that calls Amazon Lex for sentiment analysis and saves the results to an Amazon DynamoDB table. Set the TTL for all records to 365 days in the future.

答案：A

解析: Option A is the most scalable solution for automating the customer survey process. Sending survey results data to an Amazon API Gateway endpoint connected to an Amazon SQS queue, and then using an AWS Lambda function to analyze sentiment and store results in an Amazon DynamoDB table, creates a serverless architecture that can easily scale to handle thousands of responses per hour.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option A is the most scalable solution for automating the customer survey process. Sending survey results data to an Amazon API Gateway endpoint connected to an Amazon SQS queue, and then using an AWS Lambda function to analyze sentiment and store results in an Amazon DynamoDB table, creates a serverless architecture that can easily scale to handle thousands of responses per hour.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

884. Question #1007A medical company wants to perform transformations on a large amount of clinical trial data that comes from several customers. The company must extract the data from a relational database that contains the customer data. Then the company will transform the data by using a series of complex rules. The company will load the data to Amazon S3 when the transformations are complete. All data must be encrypted where it is processed before the company stores the data in Amazon S3. All data must be encrypted by using customer-specific keys. Which solution will meet these requirements with the LEAST amount of operational effort?

- A. Create one AWS Glue job for each customer. Attach a security configuration to each job that uses server-side encryption with Amazon S3 managed keys (SSE-S3) to encrypt the data.
- B. Create one Amazon EMR cluster for each customer. Attach a security configuration to each cluster that uses client-side encryption with a custom client-side root key (CSE-Custom) to encrypt the data.
- C. Create one AWS Glue job for each customer. Attach a security configuration to each job that uses client-side encryption with AWS KMS managed keys (CSE-KMS) to encrypt the data.

D. Create one Amazon EMR cluster for each customer. Attach a security configuration to each cluster that uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt the data.

答案：C

解析：To meet the medical company's requirements for processing and encrypting clinical trial data with the least operational effort, I recommend the following solution:

1. Use AWS Glue for ETL (Extract, Transform, Load) processing:
 - AWS Glue is a fully managed ETL service that can handle complex data transformations.
 - It can connect to various data sources, including relational databases.
 - Glue supports writing transformed data directly to Amazon S3.
2. Implement customer-specific encryption using AWS Key Management Service (KMS):
 - Create customer-managed KMS keys for each customer.
 - Configure AWS Glue jobs to use these customer-specific KMS keys for data encryption.
3. Set up the ETL process:
 - Create AWS Glue crawlers to catalog the source relational database.
 - Develop Glue ETL jobs to extract data from the source, apply the complex transformation rules, and load the results to S3.
 - Configure the Glue jobs to use the appropriate customer-specific KMS key for encrypting data during processing and when writing to S3.
4. Use S3 bucket policies and encryption:
 - Configure the destination S3 buckets to enforce encryption using the customer-specific KMS keys.
 - Implement bucket policies to ensure that only encrypted data can be uploaded.
5. Automate the workflow:
 - Use AWS Glue workflows to orchestrate the entire ETL process, including crawling, transformation, and data loading. This solution minimizes operational effort by leveraging fully managed AWS services. It ensures data is encrypted during processing and storage using customer-specific keys, meeting the company's security requirements.
 - Best practices to consider:
 1. Implement least privilege access for all IAM roles and policies associated with the Glue jobs and S3 buckets.
 2. Use VPC endpoints for Glue and S3 to enhance network security.
 3. Enable AWS CloudTrail and Amazon CloudWatch logs for auditing and monitoring the ETL process.
 4. Regularly rotate the customer-specific KMS keys as per your security policies.
 5. Implement data validation checks in the Glue jobs

to ensure data integrity. [1] [Protecting data with encryption – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>) [3] [Encryption best practices for Amazon S3 – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/s3.html>) [6] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>)

解析: To meet the medical company's requirements for processing and encrypting clinical trial data with the least operational effort, I recommend the following solution:

1. Use AWS Glue for ETL (Extract, Transform, Load) processing:
 - AWS Glue is a fully managed ETL service that can handle complex data transformations.
 - It can connect to various data sources, including relational databases.
 - Glue supports writing transformed data directly to Amazon S3.
2. Implement customer-specific encryption using AWS Key Management Service (KMS):
 - Create customer-managed KMS keys for each customer.
 - Configure AWS Glue jobs to use these customer-specific KMS keys for data encryption.
3. Set up the ETL process:
 - Create AWS Glue crawlers to catalog the source relational database.
 - Develop Glue ETL jobs to extract data from the source, apply the complex transformation rules, and load the results to S3.
 - Configure the Glue jobs to use the appropriate customer-specific KMS key for encrypting data during processing and when writing to S3.
4. Use S3 bucket policies and encryption:
 - Configure the destination S3 buckets to enforce encryption using the customer-specific KMS keys.
 - Implement bucket policies to ensure that only encrypted data can be uploaded.
5. Automate the workflow:
 - Use AWS Glue workflows to orchestrate the entire ETL process, including crawling, transformation, and data loading. This solution minimizes operational effort by leveraging fully managed AWS services. It ensures data is encrypted during processing and storage using customer-specific keys, meeting the company's security requirements.
 - Best practices to consider:
 1. Implement least privilege access for all IAM roles and policies associated with the Glue jobs and S3 buckets.
 2. Use VPC endpoints for Glue and S3 to enhance network security.
 3. Enable AWS CloudTrail and Amazon CloudWatch logs for auditing and monitoring the ETL process.

process.

- 4. Regularly rotate the customer-specific KMS keys as per your security policies.
- 5. Implement data validation checks in the Glue jobs to ensure data integrity.

[1] [Protecting data with encryption – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>)

[3] [Encryption best practices for Amazon S3 – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/s3.html>)

[6] [Amazon S3 FAQs – Cloud Object Storage – AWS] (<https://aws.amazon.com/s3/faqs/>)

885. Question #1008 A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics application is highly resilient and is designed to run in stateless mode. The company notices that 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?

- A. Create an Amazon Machine Image (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 across the two EC2 instances.
- B. Create an Amazon Machine Image (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. 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 is more than 75%.
- D. Create an Amazon Machine Image (AMI) of the web application. Apply the AMI to a launch template. Create an Auto Scaling group that includes the launch template. Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

答案：D

解析：Option D is the most cost-effective solution for scaling the web analytics application seamlessly. By creating an Auto Scaling group with a launch template that uses a Spot Fleet, the application can handle increased load during busy times without incurring the higher costs of

On-Demand Instances. Attaching an Application Load Balancer to the Auto Scaling group ensures that traffic is distributed evenly across instances.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the most cost-effective solution for scaling the web analytics application seamlessly. By creating an Auto Scaling group with a launch template that uses a Spot Fleet, the application can handle increased load during busy times without incurring the higher costs of On-Demand Instances. Attaching an Application Load Balancer to the Auto Scaling group ensures that traffic is distributed evenly across instances.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

886. Question #1009 A company runs an environment where data is stored in an Amazon S3 bucket. The objects are accessed frequently throughout the day. The company has strict data encryption requirements for data that is stored in the S3 bucket. The company currently uses AWS Key Management Service (AWS KMS) for encryption. The company wants to optimize costs associate

- A. Use server-side encryption with Amazon S3 managed keys (SSE-S3).
- B. Use an S3 Bucket Key for server-side encryption with AWS KMS keys (SSE-KMS) on the new objects.
- C. Use client-side encryption with AWS KMS customer managed keys.
- D. Use server-side encryption with customer-provided keys (SSE-C) stored in AWS KMS.

答案: B

解析: Option B is the solution that optimizes costs associated with encrypting S3 objects without making additional calls to AWS KMS. Using an S3 Bucket Key for server-side encryption with AWS KMS keys (SSE-KMS) on new objects allows for the use of AWS KMS for encryption management while reducing the overhead of individual encryption calls.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option B is the solution that optimizes costs associated with encrypting S3 objects without making additional calls to AWS KMS. Using

an S3 Bucket Key for server-side encryption with AWS KMS keys (SSE-KMS) on new objects allows for the use of AWS KMS for encryption management while reducing the overhead of individual encryption calls.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

887. Question #1012A company has a three-tier web application that processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer. The processing tier consists of EC2 instances. The company decoupled the web tier and processing tier by using Amazon Simple Queue Service (Amazon SQS). The storage layer uses Amazon DynamoDB. At peak times, some users report order processing delays and halls. The company has noticed that during these delays, the EC2 instances are running at 100% CPU usage, and the SQS queue fills up. The peak times are variable and unpredictable. The company needs to improve the performance of the application. Which solution will meet these requirements?

- A. Use scheduled scaling for Amazon EC2 Auto Scaling to scale out the processing tier instances for the duration of peak usage times. Use the CPU Utilization metric to determine when to scale.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier. Use target utilization as a metric to determine when to scale.
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier. Use HTTP latency as a metric to determine when to scale.
- D. Use an Amazon EC2 Auto Scaling target tracking policy to scale out the processing tier instances. Use the ApproximateNumberOfMessages attribute to determine when to scale.

答案：D

解析：Option D is the solution that will improve the performance of the application during peak times. Using an Amazon EC2 Auto Scaling target tracking policy and scaling out the processing tier instances based on the ApproximateNumberOfMessages attribute in the SQS queue allows the system to dynamically adjust to the workload, reducing order processing delays and queue buildup.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option D is the solution that will improve the performance of the application during peak times. Using an Amazon EC2 Auto Scaling target tracking policy and scaling out the processing tier instances based on the ApproximateNumberOfMessages attribute in the SQS queue allows the system to dynamically adjust to the workload, reducing order processing delays and queue buildup.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

888. Question #1013 A company's production environment consists of Amazon EC2 On-Demand Instances that run constantly between Monday and Saturday. The instances must run for only 12 hours on Sunday and cannot tolerate interruptions. The company wants to cost-optimize the production environment. Which solution will meet these requirements MOST cost-effectively?

- A. Purchase Scheduled Reserved Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved
- B. Purchase Convertible Reserved Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved
- C. Use Spot Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved Instances for the EC2
- D. Use Spot Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Convertible Reserved Instances for the EC2

答案：A

解析: Option A is the most cost-effective solution for the company's production environment. Purchasing Scheduled Reserved Instances for the EC2 instances that run for only 12 hours on Sunday and Standard Reserved Instances for the instances that run constantly between Monday and Saturday optimizes costs while ensuring minimal interruptions.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析: Option A is the most cost-effective solution for the company's production environment. Purchasing Scheduled Reserved Instances for the EC2 instances that run for only 12 hours on Sunday and Standard Reserved Instances for the instances that run constantly between Monday and Saturday optimizes costs while ensuring minimal interruptions.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

889. Question #1014 A digital image processing company wants to migrate its on-premises monolithic application to the AWS Cloud. The company processes thousands of images and generates large files as part of the processing workflow. The company needs a solution to manage the growing number of image processing jobs. The solution must also reduce the manual tasks in the image processing workflow. The company does not want to manage the underlying infrastructure of the solution. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 Spot Instances to process the images. Configure Amazon Simple Queue Service (Amazon SQS) to orchestrate the workflow. Store the processed files in Amazon Elastic File System (Amazon EFS).
- B. Use AWS Batch jobs to process the images. Use AWS Step Functions to orchestrate the workflow. Store the processed files in an Amazon S3 bucket.
- C. Use AWS Lambda functions and Amazon EC2 Spot Instances to process the images. Store the processed files in Amazon FSx.
- D. Deploy a group of Amazon EC2 instances to process the images. Use AWS Step Functions to orchestrate the workflow. Store the processed files in an Amazon Elastic Block Store (Amazon EBS) volume.

答案：B

解析：Option B is the solution that requires the least operational overhead. Using AWS Batch jobs to process images, AWS Step Functions to orchestrate the workflow, and storing processed files in an Amazon S3 bucket eliminates the need for managing underlying infrastructure and reduces manual tasks in the image processing workflow.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the solution that requires the least operational overhead. Using AWS Batch jobs to process images, AWS Step Functions to orchestrate the workflow, and storing processed files in an Amazon S3 bucket eliminates the need for managing underlying infrastructure and reduces manual tasks in the image processing workflow.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

890. Question #1015 A company's image-hosting website gives users around the world the ability to upload, view, and download images from their mobile devices. The company currently hosts the static website in an Amazon S3 bucket. Because of the website's growing popularity, the website's performance has decreased. Users have reported latency issues when they upload and download images. The company must improve the performance of the website. Which solution will meet these requirements with the LEAST implementation effort?

- A. Configure an Amazon CloudFront distribution for the S3 bucket to improve the download performance. Enable S3 Transfer Acceleration to improve the upload performance.
- B. Configure Amazon EC2 instances of the right sizes in multiple AWS Regions. Migrate the application to the EC2 instances. Use an Application Load Balancer to distribute the website traffic equally among the EC2 instances. Configure AWS Global Accelerator to address global demand with low latency.
- C. Configure an Amazon CloudFront distribution that uses the S3 bucket as an origin to improve the download performance. Configure the application to use CloudFront to upload images to improve the upload performance. Create S3 buckets in multiple AWS Regions. Configure replication rules for the buckets to replicate users' data based on the users' location. Redirect downloads to the S3 bucket that is closest to
- D. Configure AWS Global Accelerator for the S3 bucket to improve network performance. Create an endpoint for the application to use Global Accelerator instead of the S3 bucket.

答案：A

解析：Option A is the solution that requires the least implementation effort to improve the website's performance. Configuring an Amazon CloudFront distribution for the S3 bucket to improve download performance and enabling S3 Transfer Acceleration to improve upload performance can be quickly implemented with minimal changes to the existing infrastructure.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option A is the solution that requires the least implementation effort to improve the website's performance. Configuring an Amazon CloudFront distribution for the S3 bucket to improve download performance and enabling S3 Transfer Acceleration to improve upload performance can be quickly implemented with minimal changes to the existing infrastructure.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

891. Question #1016 A company runs an application in a private subnet behind an Application Load Balancer (ALB) in a VPC. The VPC has a NAT gateway and an internet gateway. The application calls the Amazon S3 API to store objects. According to the company's security policy, traffic from the application must not travel across the internet. Which solution will meet these requirements MOST cost-effectively?

- A. Configure an S3 interface endpoint. Create a security group that allows outbound traffic to Amazon S3.
- B. Configure an S3 gateway endpoint. Update the VPC route table to use the endpoint.
- C. Configure an S3 bucket policy to allow traffic from the Elastic IP address that is assigned to the NAT gateway.
- D. Create a second NAT gateway in the same subnet where the legacy application is deployed. Update the VPC route table to use the second NAT gateway.

答案：B

解析：Option B is the most cost-effective solution to meet the company's security policy. Configuring an S3 gateway endpoint and updating the VPC route table to use the endpoint allows traffic from the application to access Amazon S3 without traversing the internet, ensuring secure and private connectivity.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Option B is the most cost-effective solution to meet the company's security policy. Configuring an S3 gateway endpoint and updating the VPC route table to use the endpoint allows traffic from the application to

access Amazon S3 without traversing the internet, ensuring secure and private connectivity.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

892. Question #1017A company has an application that runs on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2 instances. The application has a UI that uses Amazon DynamoDB and data services that use Amazon S3 as part of the application deployment. The company must ensure that the EKS Pods for the UI can access only Amazon DynamoDB and that the EKS Pods for the data services can access only Amazon S3. The company uses AWS Identity and Access Management (IAM). Which solution meets these requirements?

- A. Create separate IAM policies for Amazon S3 and DynamoDB access with the required permissions. Attach both IAM policies to the EC2 instance profile. Use role-based access control (RBAC) to control access to Amazon S3 or DynamoDB for the respective EKS Pods.
- B. Create separate IAM policies for Amazon S3 and DynamoDB access with the required permissions. Attach the Amazon S3 IAM policy directly to the EKS Pods for the data services and the DynamoDB policy to the EKS Pods for the UI.
- C. Create separate Kubernetes service accounts for the UI and data services to assume an IAM role. Attach the AmazonS3FullAccess policy to the data services account and the AmazonDynamoDBFullAccess policy to the UI service account.
- D. Create separate Kubernetes service accounts for the UI and data services to assume an IAM role. Use IAM Role for Service Accounts (IRSA) to provide access to the EKS Pods for the UI to Amazon S3 and the EKS Pods for the data services to DynamoDB

答案：D

解析：To ensure that the EKS Pods for the UI can access only Amazon DynamoDB and the EKS Pods for the data services can access only Amazon S3, while using AWS Identity and Access Management (IAM), the best solution is to use IAM Roles for Service Accounts (IRSA). Here's a step-by-step guide to implement this solution:

1. **Enable IRSA for your

EKS cluster** – Navigate to the Amazon EKS console – Select your cluster – Enable IRSA if not already enabled 2. **Create IAM roles with least privilege** – Create an IAM role for UI pods with permissions to access DynamoDB – Create another IAM role for data service pods with permissions to access S3 – Ensure each role has only the necessary permissions for its specific use case 3. **Create Kubernetes service accounts** – Create a service account for UI pods – Create another service account for data service pods – Annotate each service account with the ARN of its corresponding IAM role 4. **Configure pod specifications** – Update your pod specifications to use the appropriate service account – Ensure UI pods use the service account linked to DynamoDB access – Ensure data service pods use the service account linked to S3 access 5. **Apply the changes** – Apply the updated configurations to your EKS cluster – Verify that the pods are using the correct service accounts 6. **Test and validate** – Deploy test pods to ensure they can access only their designated AWS services – Confirm that UI pods can access DynamoDB but not S3 – Confirm that data service pods can access S3 but not DynamoDB By following these steps, you'll implement a secure solution that adheres to the principle of least privilege, ensuring that each pod has access only to the AWS services it needs. This approach using IRSA provides fine-grained access control and improves the overall security posture of your EKS deployment. Sources [1] [Using service-linked roles for Amazon EKS – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/userguide/using-service-linked-roles.html>) [3] [What is Amazon EKS? – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html>) [6] [Welcome – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/APIReference>Welcome.html>)

解析: To ensure that the EKS Pods for the UI can access only Amazon DynamoDB and the EKS Pods for the data services can access only Amazon S3, while using AWS Identity and Access Management (IAM), the best solution is to use IAM Roles for Service Accounts (IRSA). Here's a step-by-step guide to implement this solution: 1. **Enable IRSA for your EKS cluster** – Navigate to the Amazon EKS console – Select your

cluster – Enable IRSA if not already enabled 2. ****Create IAM roles with least privilege**** – Create an IAM role for UI pods with permissions to access DynamoDB – Create another IAM role for data service pods with permissions to access S3 – Ensure each role has only the necessary permissions for its specific use case 3. ****Create Kubernetes service accounts**** – Create a service account for UI pods – Create another service account for data service pods – Annotate each service account with the ARN of its corresponding IAM role 4. ****Configure pod specifications**** – Update your pod specifications to use the appropriate service account – Ensure UI pods use the service account linked to DynamoDB access – Ensure data service pods use the service account linked to S3 access 5. ****Apply the changes**** – Apply the updated configurations to your EKS cluster – Verify that the pods are using the correct service accounts 6. ****Test and validate**** – Deploy test pods to ensure they can access only their designated AWS services – Confirm that UI pods can access DynamoDB but not S3 – Confirm that data service pods can access S3 but not DynamoDB By following these steps, you'll implement a secure solution that adheres to the principle of least privilege, ensuring that each pod has access only to the AWS services it needs. This approach using IRSA provides fine-grained access control and improves the overall security posture of your EKS deployment. Sources [1] [Using service-linked roles for Amazon EKS – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/userguide/using-service-linked-roles.html>) [3] [What is Amazon EKS? – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html>) [6] [Welcome – Amazon EKS] (<https://docs.aws.amazon.com/eks/latest/APIReference>Welcome.html>)

893. Question #1018 A company needs to give a globally distributed development team secure access to the company's AWS resources in a way that complies with security policies. The company currently uses an on-premises Active Directory for internal authentication. The company uses AWS Organizations to manage multiple AWS accounts that support multiple projects. The company needs a solution to integrate with the

existing infrastructure to provide centralized identity management and access control. Which solution will meet these requirements with the LEAST operational overhead?

- A. Set up AWS Directory Service to create an AWS managed Microsoft Active Directory on AWS. Establish a trust relationship with the on-premises Active Directory. Use IAM roles that are assigned to Active Directory groups to access AWS resources within the company's AWS accounts.
- B. Create an IAM user for each developer. Manually manage permissions for each IAM user based on each user's involvement with each project. Enforce multi-factor authentication (MFA) as an additional layer of security.
- C. Use AD Connector in AWS Directory Service to connect to the on-premises Active Directory. Integrate AD Connector with AWS IAM Identity Center. Configure permissions sets to give each AD group access to specific AWS accounts and resources.
- D. Use Amazon Cognito to deploy an identity federation solution. Integrate the identity federation solution with the on-premises Active Directory. Use Amazon Cognito to provide access tokens for developers to access AWS accounts and resources.

答案：C

解析：Option C is the solution that requires the least operational overhead. Using AD Connector in AWS Directory Service to connect to the on-premises Active Directory and integrating it with AWS IAM Identity Center allows for centralized identity management and access control while leveraging the existing infrastructure.

答案与解析供参考，目前还在修正中，如有不同意见，欢迎留言，谢谢、

解析：Option C is the solution that requires the least operational overhead. Using AD Connector in AWS Directory Service to connect to the on-premises Active Directory and integrating it with AWS IAM Identity Center allows for centralized identity management and access control while leveraging the existing infrastructure.

答案与解析供参考，目前还在修正中，如有不同意见，欢迎留言，谢谢、

894. Question #1019 A company is developing an application in the AWS Cloud. The application's HTTP API contains critical information that is

published in Amazon API Gateway. The critical information must be accessible from only a limited set of trusted IP addresses that belong to the company's internal network. Which solution will meet these requirements?

- A. Set up an API Gateway private integration to restrict access to a predefined set of IP addresses.
- B. Create a resource policy for the API that denies access to any IP address that is not specifically allowed.
- C. Directly deploy the API in a private subnet. Create a network ACL. Set up rules to allow the traffic from specific IP addresses.
- D. Modify the security group that is attached to API Gateway to allow inbound traffic from only the trusted IP addresses.

答案：B

解析：Option B is the solution that meets the requirements. Creating a resource policy for the API that denies access to any IP address that is not specifically allowed ensures that only a limited set of trusted IP addresses can access the critical information published in Amazon API Gateway. 答案与解析供参考，目前还在修正中，如有不同意见，欢迎留言，谢谢、

解析：Option B is the solution that meets the requirements. Creating a resource policy for the API that denies access to any IP address that is not specifically allowed ensures that only a limited set of trusted IP addresses can access the critical information published in Amazon API Gateway. 答案与解析供参考，目前还在修正中，如有不同意见，欢迎留言，谢谢、

[多选题]

1. Question #1A 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?

- 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.

答案：AC

解析：Options A and C are the correct combination of steps to securely integrate Amazon S3 with the application. Creating an Amazon Cognito identity pool to generate secure Amazon S3 access tokens (Option A) and creating an Amazon S3 VPC endpoint in the same VPC where the application is hosted (Option C) ensure secure access to S3 resources without exposing them to the public internet.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options A and C are the correct combination of steps to securely integrate Amazon S3 with the application. Creating an Amazon Cognito identity pool to generate secure Amazon S3 access tokens (Option A) and creating an Amazon S3 VPC endpoint in the same VPC where the application is hosted (Option C) ensure secure access to S3 resources without exposing them to the public internet.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

2. Question #18An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and

compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket. A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically. Which combination of actions will meet these requirements? (Choose two.)

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

答案：AB

解析：The combination of using Amazon S3 event notifications to trigger an SQS queue (A) and configuring Lambda to process messages from the SQS queue (B) creates a durable and stateless solution for automatically processing images. When an image is uploaded to the S3 bucket, it triggers a notification that sends a message to the SQS queue. Lambda is then invoked to process each message, ensuring that the image is compressed and stored in the designated S3 bucket.

解析：The combination of using Amazon S3 event notifications to trigger an SQS queue (A) and configuring Lambda to process messages from the SQS queue (B) creates a durable and stateless solution for automatically

processing images. When an image is uploaded to the S3 bucket, it triggers a notification that sends a message to the SQS queue. Lambda is then invoked to process each message, ensuring that the image is compressed and stored in the designated S3 bucket.

3. Question #44A 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.)

- 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.

答案：AB

解析：Enabling versioning on the S3 bucket ensures that all versions of the objects are stored, allowing the company to recover from accidental deletions. Enabling MFA Delete adds an extra layer of security by requiring MFA authentication before any object version can be permanently deleted. These two options together provide robust protection against accidental deletion without affecting the data access patterns.

解析：Enabling versioning on the S3 bucket ensures that all versions of the objects are stored, allowing the company to recover from accidental deletions. Enabling MFA Delete adds an extra layer of security by requiring MFA authentication before any object version can be permanently deleted. These two options together provide robust protection against accidental deletion without affecting the data access patterns.

4. Question #45A 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 metadataThe company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest

the corresponding data unless the company manually reruns the job. Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

- A. Deploy the Lambda function in multiple Availability Zones
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.
- C. Increase the CPU and memory that are allocated to the Lambda function.
- D. Increase provisioned throughput for the Lambda function.
- E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

答案：BE

解析：The issue with the current data ingestion workflow is the occasional failure of the Lambda function to ingest data due to network connectivity issues. By creating an Amazon SQS queue and subscribing it to the SNS topic (Option B), the data notifications can be queued, ensuring that no data is lost during network outages. Modifying the Lambda function to read from the SQS queue (Option E) allows the function to process any queued data as soon as the network connectivity issue is resolved, without the need for manual intervention. This combination of actions improves the reliability and resilience of the ingestion workflow, ensuring that all data is ingested in the future.

解析：The issue with the current data ingestion workflow is the occasional failure of the Lambda function to ingest data due to network connectivity issues. By creating an Amazon SQS queue and subscribing it to the SNS topic (Option B), the data notifications can be queued, ensuring that no data is lost during network outages. Modifying the Lambda function to read from the SQS queue (Option E) allows the function to process any queued data as soon as the network connectivity issue is resolved, without the need for manual intervention. This combination of actions improves the reliability and resilience of the ingestion workflow, ensuring that all data is ingested in the future.

5. Question #51A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to

extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning. Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

- A. Configure the application to send the data to Amazon Kinesis Data Firehose.
- B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
- E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

答案：BD

解析：The architect should create an AWS Lambda function that queries the application's API for the shipping statistics (Option D). The Lambda function can then format the data into an HTML format and use Amazon Simple Email Service (Option B) to send the report via email. This combination ensures that the process is automated and sends the report in the required format to the specified email addresses.

解析：The architect should create an AWS Lambda function that queries the application's API for the shipping statistics (Option D). The Lambda function can then format the data into an HTML format and use Amazon Simple Email Service (Option B) to send the report via email. This combination ensures that the process is automated and sends the report in the required format to the specified email addresses.

6. Question #92A 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.)

- 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.

答案：AC

解析：To provide secure access to the S3 bucket, the architect should configure a VPC gateway endpoint for Amazon S3 within the VPC (Option A). This allows the EC2 instances to access S3 without traversing the internet. Additionally, creating a bucket policy that limits access to only the application tier running in the VPC (Option C) ensures that the S3 bucket is only accessible to the authorized instances within the VPC, providing the necessary security for sensitive user information.

解析：To provide secure access to the S3 bucket, the architect should configure a VPC gateway endpoint for Amazon S3 within the VPC (Option A). This allows the EC2 instances to access S3 without traversing the internet. Additionally, creating a bucket policy that limits access to only the application tier running in the VPC (Option C) ensures that the S3 bucket is only accessible to the authorized instances within the VPC, providing the necessary security for sensitive user information.

7. Question #73A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access. Which combination of steps should the solutions architect take to meet these

requirements? (Choose two.)

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

答案：CD

解析：Option C is correct because it configures the bastion host's security group to allow inbound access from the external IP range of the company, which is necessary for the on-premises network to establish a connection over the internet. Option D is also correct as it sets up the application instances' security group to allow inbound SSH access only from the private IP address of the bastion host, ensuring secure access from the bastion host to the application servers within the VPC.

解析：Option C is correct because it configures the bastion host's security group to allow inbound access from the external IP range of the company, which is necessary for the on-premises network to establish a connection over the internet. Option D is also correct as it sets up the application instances' security group to allow inbound SSH access only from the private IP address of the bastion host, ensuring secure access from the bastion host to the application servers within the VPC.

8. Question #74A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company. How should security groups be configured in

this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

答案：AC

解析：Option A is correct because it allows inbound traffic on port 443 (HTTPS) for the web tier, which is necessary for the web application to receive incoming requests from clients. Option C is also correct as it permits the database tier to accept inbound traffic on port 1433 (the default port for Microsoft SQL Server) from the web tier, enabling the web application to connect to the database.

解析：Option A is correct because it allows inbound traffic on port 443 (HTTPS) for the web tier, which is necessary for the web application to receive incoming requests from clients. Option C is also correct as it permits the database tier to accept inbound traffic on port 1433 (the default port for Microsoft SQL Server) from the web tier, enabling the web application to connect to the database.

9. Question #102A 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.)

- 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.

答案：BE

解析：To automate the migration of the on-premises SFTP server to AWS, a solutions architect should take the following two steps: 1. B. Install an AWS DataSync agent in the on-premises data center. 2. E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server. Here's why these steps are the most appropriate for this scenario: 1. Installing an AWS DataSync agent in the on-premises data center allows for efficient and secure transfer of data from the existing NFS-based file system to AWS. DataSync is designed for large-scale data transfers and can handle the 200 GB of data mentioned in the question. 2. Creating a suitable location configuration for the on-premises SFTP server using AWS DataSync enables the service to properly identify and access the source data. This step is crucial for setting up the transfer task correctly. These steps automate the data transfer process, reducing manual effort and potential for errors. After the data is transferred, you can set up the EC2 instance with the Amazon EFS file system to host the new SFTP server. Additional considerations:

- Ensure that the EC2 instance is launched in the same Availability Zone as the EFS file system for optimal performance.
- Configure appropriate security groups and network access controls for the EC2 instance and EFS file system.
- After the data transfer is complete, set up and configure the SFTP server on the EC2 instance to use the EFS file system as its storage backend.
- Implement proper access controls and encryption for the data stored in the EFS file system.
- Consider using AWS Transfer for SFTP as a managed alternative to running your own SFTP server on EC2, which could simplify management and improve scalability.

Sources [1] [Migrate an on-premises SFTP server to AWS using AWS Transfer for SFTP – AWS Prescriptive

Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html>) [3] [Configuring AWS DataSync transfers with an NFS file server – AWS DataSync] (<https://docs.aws.amazon.com/datasync/latest/userguide/create-nfs-location.html>) [6] [Using AWS DataSync to transfer data – Amazon Elastic File System] (<https://docs.aws.amazon.com/efs/latest/ug/trnsfr-data-using-datasync.html>)

解析: To automate the migration of the on-premises SFTP server to AWS, a solutions architect should take the following two steps: 1. B. Install an AWS DataSync agent in the on-premises data center. 2. E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server. Here's why these steps are the most appropriate for this scenario: 1. Installing an AWS DataSync agent in the on-premises data center allows for efficient and secure transfer of data from the existing NFS-based file system to AWS. DataSync is designed for large-scale data transfers and can handle the 200 GB of data mentioned in the question. 2. Creating a suitable location configuration for the on-premises SFTP server using AWS DataSync enables the service to properly identify and access the source data. This step is crucial for setting up the transfer task correctly. These steps automate the data transfer process, reducing manual effort and potential for errors. After the data is transferred, you can set up the EC2 instance with the Amazon EFS file system to host the new SFTP server. Additional considerations: – Ensure that the EC2 instance is launched in the same Availability Zone as the EFS file system for optimal performance. – Configure appropriate security groups and network access controls for the EC2 instance and EFS file system. – After the data transfer is complete, set up and configure the SFTP server on the EC2 instance to use the EFS file system as its storage backend. – Implement proper access controls and encryption for the data stored in the EFS file system. – Consider using AWS Transfer for SFTP as a managed alternative to running your own SFTP server on EC2, which could simplify management and improve scalability. Sources [1] [Migrate an on-premises SFTP server to AWS using AWS Transfer for SFTP – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html>)

[rns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html](#) [3] [Configuring AWS DataSync transfers with an NFS file server – AWS DataSync] (<https://docs.aws.amazon.com/datasync/latest/userguide/create-nfs-location.html>) [6] [Using AWS DataSync to transfer data – Amazon Elastic File System] (<https://docs.aws.amazon.com/efs/latest/ug/trnsfr-data-using-datasync.html>)

10. Question #104A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website. Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.

答案：AC

解析：The correct answers are A and C. AWS Shield Advanced provides DDoS protection for applications running on AWS, including protecting against large-scale attacks that come from thousands of IP addresses. By using AWS Shield Advanced, the architect can ensure that the website remains protected against DDoS attacks. Additionally, Amazon CloudFront can be used to distribute the website's content globally, which not only improves the user experience by reducing latency but also provides additional layers of security and DDoS protection. Amazon GuardDuty (Option B) is a threat detection service that does not block attacks automatically. Using AWS Lambda (Option D) to modify network ACLs would not be a scalable or efficient solution for handling a large-scale DDoS

attack. While using EC2 Spot Instances (Option E) can be cost-effective, it does not directly contribute to DDoS protection and could introduce availability risks due to instance termination.

解析: The correct answers are A and C. AWS Shield Advanced provides DDoS protection for applications running on AWS, including protecting against large-scale attacks that come from thousands of IP addresses. By using AWS Shield Advanced, the architect can ensure that the website remains protected against DDoS attacks. Additionally, Amazon CloudFront can be used to distribute the website's content globally, which not only improves the user experience by reducing latency but also provides additional layers of security and DDoS protection. Amazon GuardDuty (Option B) is a threat detection service that does not block attacks automatically. Using AWS Lambda (Option D) to modify network ACLs would not be a scalable or efficient solution for handling a large-scale DDoS attack. While using EC2 Spot Instances (Option E) can be cost-effective, it does not directly contribute to DDoS protection and could introduce availability risks due to instance termination.

11. Question #110A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website. The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads. Which combination of actions should the solutions architect take to meet these requirements? (Choose two.)

- 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 Amazon S3 through the use of a pre-signed URL.
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

答案: CD

解析: To improve performance and reduce coupling, the architect should configure the application to allow users to upload images directly to Amazon S3 using pre-signed URLs (Option C). This offloads the image upload process from the EC2 instances to the users' browsers, reducing server load. Additionally, configuring S3 Event Notifications to trigger an AWS Lambda function for image resizing (Option D) ensures that resizing occurs asynchronously, without delaying the user's upload process. This combination minimizes operational overhead and improves the user experience. 答案应该是CD

解析: To improve performance and reduce coupling, the architect should configure the application to allow users to upload images directly to Amazon S3 using pre-signed URLs (Option C). This offloads the image upload process from the EC2 instances to the users' browsers, reducing server load. Additionally, configuring S3 Event Notifications to trigger an AWS Lambda function for image resizing (Option D) ensures that resizing occurs asynchronously, without delaying the user's upload process. This combination minimizes operational overhead and improves the user experience. 答案应该是CD

12. Question #116A 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 a new 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.)

- 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.

答案：AD

解析：The combination of changes that meets the requirements with the least operational overhead is to configure Amazon CloudFront in front of the website (Option A) and to create the new website and an Amazon S3 bucket, deploying the website on the S3 bucket with static website hosting enabled (Option D). CloudFront will provide global content delivery and HTTPS functionality, enhancing security with minimal configuration. S3 with static website hosting is a scalable and low-maintenance solution for serving static content, eliminating the need for a CMS and reducing operational overhead.

解析：The combination of changes that meets the requirements with the least operational overhead is to configure Amazon CloudFront in front of the website (Option A) and to create the new website and an Amazon S3 bucket, deploying the website on the S3 bucket with static website hosting enabled (Option D). CloudFront will provide global content delivery and HTTPS functionality, enhancing security with minimal configuration. S3 with static website hosting is a scalable and low-maintenance solution for serving static content, eliminating the need for a CMS and reducing operational overhead.

13. Question #125A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available. Which combination of configuration options will meet these requirements? (Choose two.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.

答案：AD

解析：The correct answers are A and D. Option A ensures that the EC2 instances and the RDS DB instance are not exposed to the public internet by launching them in private subnets. Option D allows the EC2 instances to access the internet for payment processing by configuring NAT gateways in the VPC, and also ensures that the Application Load Balancer is not exposed to the public internet by deploying it in a private subnet.

答案应该是AD

解析：The correct answers are A and D. Option A ensures that the EC2 instances and the RDS DB instance are not exposed to the public internet by launching them in private subnets. Option D allows the EC2 instances to access the internet for payment processing by configuring NAT gateways in the VPC, and also ensures that the Application Load Balancer is not exposed to the public internet by deploying it in a private subnet.

答案应该是AD

14. Question #129A 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.)

- 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).

答案：AE

解析：The correct answers are A and E. Migrating the PostgreSQL database to Amazon Aurora can reduce the operational overhead of maintaining the database. AWS Fargate, which is a part of Amazon ECS, allows the company to run containers without managing the underlying infrastructure, which can improve the scalability and efficiency of the web application.

解析：The correct answers are A and E. Migrating the PostgreSQL database to Amazon Aurora can reduce the operational overhead of maintaining the database. AWS Fargate, which is a part of Amazon ECS, allows the company to run containers without managing the underlying infrastructure, which can improve the scalability and efficiency of the web application.

15. Question #136A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database. Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

- A. Create an ongoing replication task.
- B. Create a database backup of the on-premises database.
- C. Create an AWS Database Migration Service (AWS DMS) replication server.
- D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

答案：AC

解析：To migrate the on-premises PostgreSQL database to Amazon Aurora PostgreSQL while keeping the on-premises database online and maintaining synchronization, a solutions architect should take the following two actions:

1. C. Create an AWS Database Migration Service (AWS DMS) replication server.
2. A. Create an ongoing replication task.

Here's why these actions are necessary:

1. Creating an AWS DMS replication server:
 - This is the core component that facilitates the migration process.
 - It acts as an intermediary between the source (on-premises) and target (Aurora) databases.
 - The replication server manages the data transfer and ensures minimal impact on the source database.
2. Creating an ongoing replication task:
 - This action sets up continuous data replication from the source to the target.
 - It ensures that any changes made to the on-premises database during and after the initial data load are captured and applied to the Aurora database.
 - This keeps the Aurora database synchronized with the on-premises database, meeting the requirement for ongoing synchronization.

These two actions together enable a live migration with minimal downtime, allowing the on-premises database to remain online and accessible throughout the process. Some additional considerations and best practices for this migration:

- Perform a thorough assessment of the source database before migration.
- Test the migration process in a non-production environment first.
- Monitor the replication process using AWS DMS's built-in monitoring tools and Amazon CloudWatch.
- Plan for a cutover strategy to switch from the on-premises database to Aurora when ready.
- Implement appropriate security measures, such as encryption in transit and at rest for your data.
- Regularly review and optimize the migration process as needed.

For the most up-to-date information on AWS DMS capabilities, limitations, and best practices, please refer to the official AWS documentation.

Sources [1] [Considering online migration options – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-databases-postgresql-ec2/considering-online-migration-options.html>)
[3] [Migrate an on-premises PostgreSQL database to Aurora PostgreSQL – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-databases-postgresql-ec2/migrating-on-premises-postgresql-database-to-aurora-postgresql.html>)

[ance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html](https://docs.aws.amazon.com/whitepapers/latest/migrating-databases-to-amazon-aurora/migrating-data.html) [6] [Migrating data – Migrating Your Databases to Amazon Aurora] (<https://docs.aws.amazon.com/whitepapers/latest/migrating-databases-to-amazon-aurora/migrating-data.html>)

解析: To migrate the on-premises PostgreSQL database to Amazon Aurora PostgreSQL while keeping the on-premises database online and maintaining synchronization, a solutions architect should take the following two actions:

1. C. Create an AWS Database Migration Service (AWS DMS) replication server.
2. A. Create an ongoing replication task.

Here's why these actions are necessary:

1. Creating an AWS DMS replication server:
 - This is the core component that facilitates the migration process.
 - It acts as an intermediary between the source (on-premises) and target (Aurora) databases.
 - The replication server manages the data transfer and ensures minimal impact on the source database.
2. Creating an ongoing replication task:
 - This action sets up continuous data replication from the source to the target.
 - It ensures that any changes made to the on-premises database during and after the initial data load are captured and applied to the Aurora database.
 - This keeps the Aurora database synchronized with the on-premises database, meeting the requirement for ongoing synchronization.

These two actions together enable a live migration with minimal downtime, allowing the on-premises database to remain online and accessible throughout the process.

Some additional considerations and best practices for this migration:

- Perform a thorough assessment of the source database before migration.
- Test the migration process in a non-production environment first.
- Monitor the replication process using AWS DMS's built-in monitoring tools and Amazon CloudWatch.
- Plan for a cutover strategy to switch from the on-premises database to Aurora when ready.
- Implement appropriate security measures, such as encryption in transit and at rest for your data.
- Regularly review and optimize the migration process as needed.

For the most up-to-date information on AWS DMS capabilities, limitations, and best practices, please refer to the official AWS documentation.

Sources [1] [Considering online migration options – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/migra>

tion-databases-postgresql-ec2/considering-online-migration-options.html)
[3] [Migrate an on-premises PostgreSQL database to Aurora PostgreSQL – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html>) [6] [Migrating data – Migrating Your Databases to Amazon Aurora] (<https://docs.aws.amazon.com/whitepapers/latest/migrating-databases-to-amazon-aurora/migrating-data.html>)

16. Question #140A 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.)

- 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.

答案: AC

解析: The correct answers are A and C. Using Spot Instances for the data ingestion layer can be cost-effective since the workload is sporadic and can be interrupted. A Compute Savings Plan can provide significant savings for the front-end and API layer, which have predictable utilization over a year.

解析: The correct answers are A and C. Using Spot Instances for the data ingestion layer can be cost-effective since the workload is sporadic and can be interrupted. A Compute Savings Plan can provide significant savings for the front-end and API layer, which have predictable utilization over a year.

17. Question #151A 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.)

- 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.

答案: AC

解析: The correct answers are A and C. Using AWS Control Tower to implement data residency guardrails can restrict access to the specified AWS Region and deny internet access. Configuring service control policies (SCPs) in AWS Organizations can also prevent VPCs from gaining internet access and restrict access to the ap-northeast-3 Region.

解析: The correct answers are A and C. Using AWS Control Tower to implement data residency guardrails can restrict access to the specified AWS Region and deny internet access. Configuring service control policies (SCPs) in AWS Organizations can also prevent VPCs from gaining internet

access and restrict access to the ap-northeast-3 Region.

18. Question #156A 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.)

- 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.

答案：AE

解析：The correct answers are A and E. Using Amazon Athena for one-time queries on the data stored in S3 allows for ad-hoc analysis without the need for a dedicated data warehouse. AWS Glue can be used to automate the data transformation and loading process into S3 in a columnar storage format like Apache Parquet, which is optimized for analytics. Amazon QuickSight can then be used to create dashboards for visualizing KPIs.

解析：The correct answers are A and E. Using Amazon Athena for one-time queries on the data stored in S3 allows for ad-hoc analysis without the need for a dedicated data warehouse. AWS Glue can be used to automate the data transformation and loading process into S3 in a columnar storage

format like Apache Parquet, which is optimized for analytics. Amazon QuickSight can then be used to create dashboards for visualizing KPIs.

19. Question #157A 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.)

- 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.

答案：DE

解析：The correct answers are D and E. Configuring an Amazon CloudWatch Logs export for the DB cluster will allow the company to keep audit logs indefinitely. Using AWS Backup to manage the automated backups provides a centralized solution to create, manage, and restore backups, including setting retention policies for 5 years.

解析：The correct answers are D and E. Configuring an Amazon CloudWatch Logs export for the DB cluster will allow the company to keep audit logs indefinitely. Using AWS Backup to manage the automated backups provides a centralized solution to create, manage, and restore backups, including setting retention policies for 5 years.

20. Question #159A 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.)

- 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.

答案：AC

解析：The correct answers are A and C. Creating a usage plan with an API key for Amazon API Gateway can help control and limit access to the API. Implementing an AWS WAF rule can provide an additional layer of security by allowing the architect to define custom rules that block or allow traffic based on criteria such as IP addresses, request rates, and other patterns that may indicate fraudulent activity.

解析：The correct answers are A and C. Creating a usage plan with an API key for Amazon API Gateway can help control and limit access to the API. Implementing an AWS WAF rule can provide an additional layer of security by allowing the architect to define custom rules that block or allow traffic based on criteria such as IP addresses, request rates, and other patterns that may indicate fraudulent activity.

21. Question #180A 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.)

- 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.

答案：BC

解析：The correct answers are B and C. AWS Shield Advanced provides protection against sophisticated DDoS attacks and can be associated with the NLB to safeguard the EC2 instances. AWS WAF (Web Application Firewall) can be used to protect Amazon API Gateway, helping to protect against web exploits like SQL injection. Together, these services offer a comprehensive security solution for the platform.

解析：The correct answers are B and C. AWS Shield Advanced provides protection against sophisticated DDoS attacks and can be associated with the NLB to safeguard the EC2 instances. AWS WAF (Web Application Firewall) can be used to protect Amazon API Gateway, helping to protect against web exploits like SQL injection. Together, these services offer a comprehensive security solution for the platform.

22. Question #187A 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.)

- 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.

答案：AD

解析：Option A is correct as Amazon RDS in Multi-AZ mode automatically creates a standby replica in a different Availability Zone which provides

data redundancy, automatic failover, and increased availability. Option D is also correct as AWS Fargate is a serverless compute engine for containers that removes the need to provision and manage servers, thus reducing the manual intervention.

解析: Option A is correct as Amazon RDS in Multi-AZ mode automatically creates a standby replica in a different Availability Zone which provides data redundancy, automatic failover, and increased availability. Option D is also correct as AWS Fargate is a serverless compute engine for containers that removes the need to provision and manage servers, thus reducing the manual intervention.

23. Question #189A 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.)

- 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.

答案: BD

解析: Option A provides protection against deletion and overwriting but does not address key rotation. Option B, with S3 Object Lock in compliance mode, ensures that objects cannot be deleted for a specified retention period, but it also does not address key rotation. Option C is incorrect because SSE-S3 keys are rotated automatically by AWS, but the

user cannot configure the rotation frequency. Option D is correct as it allows for the use of AWS KMS to manage keys with the ability to configure an annual rotation, meeting the requirement for automatic key rotation.

解析: Option A provides protection against deletion and overwriting but does not address key rotation. Option B, with S3 Object Lock in compliance mode, ensures that objects cannot be deleted for a specified retention period, but it also does not address key rotation. Option C is incorrect because SSE-S3 keys are rotated automatically by AWS, but the user cannot configure the rotation frequency. Option D is correct as it allows for the use of AWS KMS to manage keys with the ability to configure an annual rotation, meeting the requirement for automatic key rotation.

24. Question #192A 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.)
- 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.

答案：BE

解析：Option B is correct as Amazon S3 can be used to store the documents and Amazon Athena can query the data stored in S3 using SQL, which is efficient for large-scale data operations. Option E is also correct as AWS Lambda can be triggered upon new document uploads, using Amazon Textract to convert documents to text and Amazon Comprehend Medical to extract medical information, which is scalable and serverless.

解析：Option B is correct as Amazon S3 can be used to store the documents and Amazon Athena can query the data stored in S3 using SQL, which is efficient for large-scale data operations. Option E is also correct as AWS Lambda can be triggered upon new document uploads, using Amazon Textract to convert documents to text and Amazon Comprehend Medical to extract medical information, which is scalable and serverless.

25. Question #197A 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.)

- 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.

答案：BE

解析：Option B is correct as AWS Elastic Beanstalk supports .NET applications and can be deployed in a Multi-AZ configuration for high availability. Option E is also correct as AWS DMS can be used to migrate the Oracle database to Oracle on Amazon RDS, which can also be deployed in a Multi-AZ configuration for high availability, without requiring significant changes to the application code.

解析：Option B is correct as AWS Elastic Beanstalk supports .NET applications and can be deployed in a Multi-AZ configuration for high availability. Option E is also correct as AWS DMS can be used to migrate the Oracle database to Oracle on Amazon RDS, which can also be deployed in a Multi-AZ configuration for high availability, without requiring significant changes to the application code.

26. Question #218A 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.)

- 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.

答案：AE

解析：Option A is correct as it involves creating a security group rule that allows inbound traffic on port 443 from any source, which is

necessary for making the web server accessible on port 443. Option E is also correct as it updates the network ACL to allow outbound responses from the web server to any destination on the ephemeral port range, which is required because network ACLs are stateless and must allow the return traffic for established connections.

解析: Option A is correct as it involves creating a security group rule that allows inbound traffic on port 443 from any source, which is necessary for making the web server accessible on port 443. Option E is also correct as it updates the network ACL to allow outbound responses from the web server to any destination on the ephemeral port range, which is required because network ACLs are stateless and must allow the return traffic for established connections.

27. Question #223A 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.)

- 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.

答案: AD

解析: To allow the Java Spring Boot application running on Amazon EKS to interact with an Amazon DynamoDB table without exposing traffic to the internet, the solutions architect should take the following steps: - Attach an IAM role with sufficient privileges (Option A) to the EKS pod. This will enable the application to use the permissions associated with the role to access DynamoDB. - Create a VPC endpoint for DynamoDB (Option D). This will ensure that the traffic between the EKS pods and DynamoDB stays within the AWS network and does not go over the public internet.

Option B is not necessary because attaching an IAM user to the EKS pod would require managing credentials within the pod, which is less secure and more complex than using an IAM role. Option C is not sufficient on its own because, while it allows outbound connectivity, it does not ensure that the traffic is private and does not go over the internet.

解析：To allow the Java Spring Boot application running on Amazon EKS to interact with an Amazon DynamoDB table without exposing traffic to the internet, the solutions architect should take the following steps: –

Attach an IAM role with sufficient privileges (Option A) to the EKS pod. This will enable the application to use the permissions associated with the role to access DynamoDB. – Create a VPC endpoint for DynamoDB (Option D). This will ensure that the traffic between the EKS pods and DynamoDB stays within the AWS network and does not go over the public internet.

Option B is not necessary because attaching an IAM user to the EKS pod would require managing credentials within the pod, which is less secure and more complex than using an IAM role. Option C is not sufficient on its own because, while it allows outbound connectivity, it does not ensure that the traffic is private and does not go over the internet.

28. Question #224A 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.)

- 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.

答案：CE

解析: To achieve high availability and fault tolerance, the company should:

- Create an Amazon Route 53 multivalue answer routing policy (Option C). This allows Route 53 to respond to DNS queries with up to eight healthy records selected at random. This ensures that traffic is distributed randomly across all running EC2 instances.
- Launch four EC2 instances with two instances in one Availability Zone and two instances in another Availability Zone (Option E). This setup provides redundancy within and across different Availability Zones, which is crucial for fault tolerance.

Option A is not suitable because a failover routing policy is designed for scenarios where you want to redirect traffic from a primary resource to a secondary resource in case of failure, rather than distributing traffic randomly among multiple resources. Option B is not ideal because a weighted routing policy is used when you want to control the traffic distribution based on predefined weights, not randomly. Option D does not provide optimal fault tolerance because having only one instance in a separate Availability Zone does not balance the traffic evenly across zones.

解析: To achieve high availability and fault tolerance, the company should:

- Create an Amazon Route 53 multivalue answer routing policy (Option C). This allows Route 53 to respond to DNS queries with up to eight healthy records selected at random. This ensures that traffic is distributed randomly across all running EC2 instances.
- Launch four EC2 instances with two instances in one Availability Zone and two instances in another Availability Zone (Option E). This setup provides redundancy within and across different Availability Zones, which is crucial for fault tolerance.

Option A is not suitable because a failover routing policy is designed for scenarios where you want to redirect traffic from a primary resource to a secondary resource in case of failure, rather than distributing traffic randomly among multiple resources. Option B is not ideal because a weighted routing policy is used when you want to control the traffic distribution based on predefined weights, not randomly. Option D does not provide optimal fault tolerance because having only one instance in a separate Availability Zone does not balance the traffic evenly across zones.

29. Question #226A 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.)

- 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.

答案：AE

解析：To create a highly scalable solution that can handle an increasing amount of data from remote devices, the solutions architect should:
– Use Amazon API Gateway (Option E) to manage and process the incoming data from the RESTful web services application. API Gateway can handle the increasing number of requests by automatically scaling and is designed to work with other AWS services like Kinesis.
– Use Amazon Kinesis Data Firehose (Option E) to automatically collect and deliver the raw data to an Amazon S3 bucket. Kinesis Data Firehose can scale to handle large amounts of data and provides a reliable way to load streaming data into S3.
Option A, AWS Glue, is a data preparation service that can be used for ETL (extract, transform, load) jobs, but it is not directly mentioned as part of the solution for handling the initial influx of data. Option B, Amazon Route 53, is a DNS web service and is not directly related to the data processing requirements described. Option C, adding more EC2 instances, could provide more capacity but does not address the

scalability in a way that minimizes operational overhead as effectively as using managed services like Kinesis Data Firehose. Option D, using Amazon SQS, could be part of a solution for queuing data, but it is not as directly suited to the data ingestion and processing needs as Kinesis Data Firehose.

解析: To create a highly scalable solution that can handle an increasing amount of data from remote devices, the solutions architect should: – Use Amazon API Gateway (Option E) to manage and process the incoming data from the RESTful web services application. API Gateway can handle the increasing number of requests by automatically scaling and is designed to work with other AWS services like Kinesis. – Use Amazon Kinesis Data Firehose (Option E) to automatically collect and deliver the raw data to an Amazon S3 bucket. Kinesis Data Firehose can scale to handle large amounts of data and provides a reliable way to load streaming data into S3. Option A, AWS Glue, is a data preparation service that can be used for ETL (extract, transform, load) jobs, but it is not directly mentioned as part of the solution for handling the initial influx of data. Option B, Amazon Route 53, is a DNS web service and is not directly related to the data processing requirements described. Option C, adding more EC2 instances, could provide more capacity but does not address the scalability in a way that minimizes operational overhead as effectively as using managed services like Kinesis Data Firehose. Option D, using Amazon SQS, could be part of a solution for queuing data, but it is not as directly suited to the data ingestion and processing needs as Kinesis Data Firehose.

30. Question #247A 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.)
- 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.

答案：CE

解析：Before implementing a read replica for an Amazon RDS for MySQL database, the solutions architect should:

- Allow long-running transactions to complete on the source DB instance (Option C).
- Long-running transactions can lock tables and prevent the creation of a read replica.
- Enable automatic backups on the source instance by setting the backup retention period to a value other than 0 (Option E).

This is a requirement for creating a read replica from the source DB instance. Enabling binlog replication (Option A) is not a prerequisite for creating a read replica in Amazon RDS. Choosing a failover priority (Option B) is relevant for Multi-AZ deployments, not for read replicas. Creating a global table (Option D) is a feature related to Amazon DynamoDB and not applicable to RDS for MySQL.

解析：Before implementing a read replica for an Amazon RDS for MySQL database, the solutions architect should:

- Allow long-running transactions to complete on the source DB instance (Option C).
- Long-running transactions can lock tables and prevent the creation of a read replica.
- Enable automatic backups on the source instance by setting the backup retention period to a value other than 0 (Option E).

This is a requirement for creating a read replica from the source DB instance. Enabling binlog replication (Option A) is not a prerequisite for creating a read replica in Amazon RDS. Choosing a failover priority (Option B) is relevant for Multi-AZ deployments, not for read replicas. Creating a global table (Option D) is a feature related to Amazon DynamoDB and not applicable to RDS for MySQL.

31. Question #256A 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.)

- 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.

答案：BD

解析：To meet the requirements for the document review application, the solutions architect should enable versioning on the bucket (Option B) and enable MFA Delete on the bucket (Option D). Versioning ensures that all versions of the documents are kept, allowing users to access previous versions if needed. MFA Delete adds an additional layer of security by requiring a multi-factor authentication (MFA) code to delete objects from the bucket, which helps prevent accidental deletions. Option A, a read-only bucket ACL, would prevent users from modifying and uploading documents, which is not consistent with the requirements. Option C, attaching an IAM policy to the bucket, is a good practice for access control but does not directly address the prevention of accidental deletions or the availability of document versions. Option E, encrypting the bucket using AWS KMS, is important for data security but is not directly related to the document versioning or deletion prevention requirements.

解析：To meet the requirements for the document review application, the solutions architect should enable versioning on the bucket (Option B) and enable MFA Delete on the bucket (Option D). Versioning ensures that all versions of the documents are kept, allowing users to access previous versions if needed. MFA Delete adds an additional layer of security by requiring a multi-factor authentication (MFA) code to delete objects from the bucket, which helps prevent accidental deletions. Option A, a read-only bucket ACL, would prevent users from modifying and uploading documents, which is not consistent with the requirements. Option C, attaching an IAM policy to the bucket, is a good practice for access control but does not directly address the prevention of accidental

deletions or the availability of document versions. Option E, encrypting the bucket using AWS KMS, is important for data security but is not directly related to the document versioning or deletion prevention requirements.

32. Question #261A 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.)

- 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 Lambda@Edge 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.

答案：AC

解析：To provide different versions of content based on the devices used by customers, the solutions architect should configure Amazon CloudFront to cache multiple versions of the content (Option A) and use a Lambda@Edge function to send specific objects based on the User-Agent header (Option C). CloudFront can cache and serve different versions of content from edge locations closer to the users, improving performance and user experience. Lambda@Edge can process incoming requests and serve the appropriate content based on the device type detected from the User-Agent header.

解析: To provide different versions of content based on the devices used by customers, the solutions architect should configure Amazon CloudFront to cache multiple versions of the content (Option A) and use a Lambda@Edge function to send specific objects based on the User-Agent header (Option C). CloudFront can cache and serve different versions of content from edge locations closer to the users, improving performance and user experience. Lambda@Edge can process incoming requests and serve the appropriate content based on the device type detected from the User-Agent header.

33. Question #263A 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.)

- 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.

答案: AD

解析: To minimize ongoing effort for maintenance and scaling without managing additional infrastructure, a solutions architect should deploy an Amazon ECS service with a Fargate launch type (Option D) and specify a desired task number level of greater than or equal to 2 (Option C).

Amazon ECS with Fargate allows the company to run containers without the need to manage servers or clusters, as Fargate is a serverless offering that automatically manages the underlying infrastructure. Additionally,

setting a desired task number ensures that the specified number of tasks is running, providing a basic level of scaling.

解析: To minimize ongoing effort for maintenance and scaling without managing additional infrastructure, a solutions architect should deploy an Amazon ECS service with a Fargate launch type (Option D) and specify a desired task number level of greater than or equal to 2 (Option C).

Amazon ECS with Fargate allows the company to run containers without the need to manage servers or clusters, as Fargate is a serverless offering that automatically manages the underlying infrastructure. Additionally, setting a desired task number ensures that the specified number of tasks is running, providing a basic level of scaling.

34. Question #276A 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.)

- 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.

答案: AD

解析: waiting...

解析: waiting...

35. Question #278A 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.)

- 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.

答案：BE

解析：Explanation: To store employee data in a hierarchical structured relationship with high-traffic query support and sensitive data protection, a solutions architect should: B. Use Amazon DynamoDB to store the employee data in hierarchies. DynamoDB is a NoSQL database service that provides fast and predictable performance with seamless scalability. It can handle hierarchical data structures and offers built-in security features to protect sensitive information. E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon SNS subscription. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. By integrating with Amazon EventBridge and SNS, the company can set up a system to receive monthly notifications if any financial information is detected, helping to meet

compliance and monitoring requirements. Option A, while it can handle structured data and provide fast query responses, does not directly address the need for hierarchical data storage or the monthly notification requirement. Option C is similar to option E but does not specify the use of SNS for notifications, which is a more suitable method for sending messages to a potentially large number of subscribers. Option D could be useful for data analysis and dashboard publishing but does not directly contribute to the storage, protection, or notification requirements specified.

解析: Explanation: To store employee data in a hierarchical structured relationship with high-traffic query support and sensitive data protection, a solutions architect should: B. Use Amazon DynamoDB to store the employee data in hierarchies. DynamoDB is a NoSQL database service that provides fast and predictable performance with seamless scalability. It can handle hierarchical data structures and offers built-in security features to protect sensitive information. E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon SNS subscription. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. By integrating with Amazon EventBridge and SNS, the company can set up a system to receive monthly notifications if any financial information is detected, helping to meet compliance and monitoring requirements. Option A, while it can handle structured data and provide fast query responses, does not directly address the need for hierarchical data storage or the monthly notification requirement. Option C is similar to option E but does not specify the use of SNS for notifications, which is a more suitable method for sending messages to a potentially large number of subscribers. Option D could be useful for data analysis and dashboard publishing but does not directly contribute to the storage, protection, or notification requirements specified.

36. Question #291A 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.)

- A. Signed cookies
- B. Signed URLs
- C. AWS AppSync
- D. JSON Web Token (JWT)
- E. AWS Secrets Manager

答案：AB

解析：Based on the requirements provided, the two services or methods that will meet the media company's needs with the least impact to users are:

- 1. Signed URLs
 - Ideal for users with custom HTTP clients that don't support cookies
 - Can be used with existing hardcoded URLs, minimizing impact on users who can't change their URLs
 - Provides secure, time-limited access to specific CloudFront content
 - Allows fine-grained control over access to individual files or sets of files
- 2. Signed cookies
 - Useful for users who can support cookies in their clients
 - Provides access to multiple restricted files without changing URLs
 - Reduces the need for URL modifications, which is beneficial for users with hardcoded URLs

These methods work well together, allowing the media company to cater to different user needs:

- Users with custom HTTP clients that don't support cookies can use signed URLs
- Users who can support cookies but have hardcoded URLs can use signed cookies

Both options integrate seamlessly with Amazon CloudFront and Amazon S3, providing a secure way to control access to the video content without significant changes to the existing infrastructure or user experience.

To implement these solutions:

1. Configure CloudFront to require signed URLs or signed cookies for access to the S3 content
2. Set up a trusted key group in CloudFront for signing URLs and cookies
3. Implement a process to generate signed URLs or cookies for authorized

users. For the most up-to-date implementation details and best practices, refer to the official AWS documentation on using signed URLs and signed cookies with CloudFront. Sources [1] [Securing your contents with CloudFront – Secure Content Delivery with Amazon CloudFront] (<https://docs.aws.amazon.com/whitepapers/latest/secure-content-delivery-amazon-cloudfront/securing-your-contents-with-cloudfront.html>) [3] [Security – Amazon CloudFront for Media] (<https://docs.aws.amazon.com/whitepapers/latest/amazon-cloudfront-media/security.html>) [6] [Amazon CloudFront for Media – Amazon CloudFront for Media] (<https://docs.aws.amazon.com/whitepapers/latest/amazon-cloudfront-media/amazon-cloudfront-media.html>)

解析: Based on the requirements provided, the two services or methods that will meet the media company's needs with the least impact to users are:

1. Signed URLs
 - Here's why these options are the most suitable:
 - Ideal for users with custom HTTP clients that don't support cookies
 - Can be used with existing hardcoded URLs, minimizing impact on users who can't change their URLs
 - Provides secure, time-limited access to specific CloudFront content
 - Allows fine-grained control over access to individual files or sets of files
 2. Signed cookies
 - Useful for users who can support cookies in their clients
 - Provides access to multiple restricted files without changing URLs
 - Reduces the need for URL modifications, which is beneficial for users with hardcoded URLs

These methods work well together, allowing the media company to cater to different user needs:

 - Users with custom HTTP clients that don't support cookies can use signed URLs
 - Users who can support cookies but have hardcoded URLs can use signed cookies

Both options integrate seamlessly with Amazon CloudFront and Amazon S3, providing a secure way to control access to the video content without significant changes to the existing infrastructure or user experience.

To implement these solutions:

 1. Configure CloudFront to require signed URLs or signed cookies for access to the S3 content
 2. Set up a trusted key group in CloudFront for signing URLs and cookies
 3. Implement a process to generate signed URLs or cookies for authorized users

For the most up-to-date implementation details and best practices, refer to the official AWS documentation on using signed URLs and signed

cookies with CloudFront. Sources [1] [Securing your contents with CloudFront – Secure Content Delivery with Amazon CloudFront] (<https://docs.aws.amazon.com/whitepapers/latest/securing-content-delivery-amazon-cloudfront/securing-your-contents-with-cloudfront.html>) [3] [Security – Amazon CloudFront for Media] (<https://docs.aws.amazon.com/whitepapers/latest/amazon-cloudfront-media/security.html>) [6] [Amazon CloudFront for Media – Amazon CloudFront for Media] (<https://docs.aws.amazon.com/whitepapers/latest/amazon-cloudfront-media/amazon-cloudfront-media.html>)

37. Question #292A 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.)
- 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.

答案：AB

解析: To create a data platform that can ingest, transform, and query real-time streaming data, a solutions architect should consider: A. Using Amazon Kinesis Data Streams to stream data, Amazon Kinesis Data Analytics to transform the data, Amazon Kinesis Data Firehose to write the transformed data to Amazon S3, and Amazon Athena to query the data. This solution leverages the full capabilities of the Kinesis suite for real-time data processing and allows for direct querying of the data in S3 using Athena. B. Using Amazon MSK to stream data, AWS Glue to transform the data, and then writing the transformed data to Amazon S3 for querying with Amazon Athena. This solution provides a managed Apache Kafka service for streaming data and uses AWS Glue for ETL (extract, transform, load) processes before querying with Athena. Both options A and B meet the requirements by providing a method to stream, transform, and query data using SQL through Amazon Athena. They offer scalable and fully managed services that integrate well for this use case.

解析: To create a data platform that can ingest, transform, and query real-time streaming data, a solutions architect should consider: A. Using Amazon Kinesis Data Streams to stream data, Amazon Kinesis Data Analytics to transform the data, Amazon Kinesis Data Firehose to write the transformed data to Amazon S3, and Amazon Athena to query the data. This solution leverages the full capabilities of the Kinesis suite for real-time data processing and allows for direct querying of the data in S3 using Athena. B. Using Amazon MSK to stream data, AWS Glue to transform the data, and then writing the transformed data to Amazon S3 for querying with Amazon Athena. This solution provides a managed Apache Kafka service for streaming data and uses AWS Glue for ETL (extract, transform, load) processes before querying with Athena. Both options A and B meet the requirements by providing a method to stream, transform, and query data using SQL through Amazon Athena. They offer scalable and fully managed services that integrate well for this use case.

38. Question #302A 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.)

- 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.

答案：AC

解析：To improve the performance and scalability of the mobile app for streaming slow-motion video clips, while minimizing operational overhead, the company should:
A. Deploy Amazon CloudFront for content delivery and caching. CloudFront is a global content delivery network (CDN) service that can cache video clips at edge locations closer to the users, reducing latency and buffering issues during playback.
C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats. Elastic Transcoder is a media transcoding service that can convert video clips into formats that are optimized for different devices and network conditions, reducing the file size and improving the playback experience without compromising quality.
Option B is not necessary for improving the performance of video streaming to mobile devices. Option D is not the most cost-effective solution, as it involves managing an Auto Scaling group of EC2 instances for content delivery and caching, which adds operational overhead. Option E is also not the most efficient solution, as it would require running EC2 instances to perform the video conversion, which is not as cost-effective or scalable as using a managed service like Elastic Transcoder.

解析: To improve the performance and scalability of the mobile app for streaming slow-motion video clips, while minimizing operational overhead, the company should: A. Deploy Amazon CloudFront for content delivery and caching. CloudFront is a global content delivery network (CDN) service that can cache video clips at edge locations closer to the users, reducing latency and buffering issues during playback. C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats. Elastic Transcoder is a media transcoding service that can convert video clips into formats that are optimized for different devices and network conditions, reducing the file size and improving the playback experience without compromising quality. Option B is not necessary for improving the performance of video streaming to mobile devices. Option D is not the most cost-effective solution, as it involves managing an Auto Scaling group of EC2 instances for content delivery and caching, which adds operational overhead. Option E is also not the most efficient solution, as it would require running EC2 instances to perform the video conversion, which is not as cost-effective or scalable as using a managed service like Elastic Transcoder.

39. Question #308A 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.)
- 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.

答案：BD

解析：To access Trusted Advisor recommendations for RDS and review the appropriate checks to reduce RDS costs, the finance team should: B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time. This allows the team to have a unified view of all the RDS instances across different accounts, making it easier to identify and implement cost-saving measures. D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances. This check can help identify RDS instances that are not being utilized effectively, which may lead to recommendations for reducing costs, such as by resizing or terminating underutilized instances. Option A is less efficient because it would require the finance team to log into each individual account to review the RDS instances. Option C is not applicable if the company is using On-Demand instances, as Reserved Instance Optimization is more relevant for reserved instances. Option E is not relevant to the scenario as it pertains to Amazon Redshift, not RDS.

解析：To access Trusted Advisor recommendations for RDS and review the appropriate checks to reduce RDS costs, the finance team should: B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time. This allows the team to have a unified view of all the RDS instances across different accounts, making it easier to identify and implement cost-saving measures. D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances. This check can help identify RDS instances that are not being utilized effectively, which may lead to recommendations for reducing costs, such as by resizing or terminating underutilized instances. Option A is less efficient because it would require the finance team to log into each individual account to review the RDS instances. Option C is not applicable if the company is using On-Demand instances, as Reserved Instance Optimization is more relevant for reserved instances. Option E

is not relevant to the scenario as it pertains to Amazon Redshift, not RDS.

40. Question #318A 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.)

- 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.

答案：AD

解析：To track and audit inventory and configuration changes in the AWS Cloud environment, a solutions architect should: A. Enable AWS CloudTrail and use it for auditing. CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. It can be used to track and audit changes to resources, including EC2 instance provisioning and security group modifications. D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It can record changes to configurations and allow you to create rules to ensure that resources are in compliance with your desired configurations. Option B, using data lifecycle policies, is more relevant to managing the lifecycle of data within services like Amazon S3, rather than auditing EC2 instances. Option C, AWS Trusted Advisor, provides recommendations to optimize AWS resources but is not designed for detailed auditing and compliance tracking. Option E, using AWS CloudFormation, is more about infrastructure as code and does not

inherently provide auditing or compliance monitoring capabilities.

解析: To track and audit inventory and configuration changes in the AWS Cloud environment, a solutions architect should: A. Enable AWS CloudTrail and use it for auditing. CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. It can be used to track and audit changes to resources, including EC2 instance provisioning and security group modifications. D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It can record changes to configurations and allow you to create rules to ensure that resources are in compliance with your desired configurations. Option B, using data lifecycle policies, is more relevant to managing the lifecycle of data within services like Amazon S3, rather than auditing EC2 instances. Option C, AWS Trusted Advisor, provides recommendations to optimize AWS resources but is not designed for detailed auditing and compliance tracking. Option E, using AWS CloudFormation, is more about infrastructure as code and does not inherently provide auditing or compliance monitoring capabilities.

41. Question #326 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.)

- 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.

答案：AB

解析：To optimize storage costs for the image hosting company's use case, the solutions architect should recommend moving assets to S3 Intelligent-Tiering after 30 days, as it will automatically move the data to the most cost-effective access tier without operational overhead, based on access patterns. Additionally, configuring an S3 Lifecycle policy to clean up incomplete multipart uploads will prevent unnecessary charges from incomplete uploads that may have been interrupted or failed. These two actions together will help maintain high availability and resiliency while reducing storage costs.

解析：To optimize storage costs for the image hosting company's use case, the solutions architect should recommend moving assets to S3 Intelligent-Tiering after 30 days, as it will automatically move the data to the most cost-effective access tier without operational overhead, based on access patterns. Additionally, configuring an S3 Lifecycle policy to clean up incomplete multipart uploads will prevent unnecessary charges from incomplete uploads that may have been interrupted or failed. These two actions together will help maintain high availability and resiliency while reducing storage costs.

42. Question #350A 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.)

- 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.

答案：AC

解析：To achieve high availability and improve the performance of the report process, the solutions architect should modify the DB instance from a Single-AZ deployment to a Multi-AZ deployment, which provides automatic failover and increased availability. Additionally, creating a read replica in a different Availability Zone and directing all reporting requests to the read replica can help offload the reporting workload from the primary DB instance, thereby improving the performance of the transactional processes. Using a read replica for reporting purposes allows the primary instance to focus on transactional workload, while the read replica can handle the less critical but resource-intensive reporting tasks.

解析：To achieve high availability and improve the performance of the report process, the solutions architect should modify the DB instance from a Single-AZ deployment to a Multi-AZ deployment, which provides automatic failover and increased availability. Additionally, creating a read replica in a different Availability Zone and directing all reporting requests to the read replica can help offload the reporting workload from the primary DB instance, thereby improving the performance of the transactional processes. Using a read replica for reporting purposes allows the primary instance to focus on transactional workload, while the read replica can handle the less critical but resource-intensive reporting tasks.

43. Question #357A 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.)

- 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.

答案：AD

解析：To ensure high availability of the storage solution for the gaming application, the solutions architect should store the static files on Amazon S3 and use Amazon CloudFront to cache objects at the edge, which will help in distributing the content globally and reducing latency. Additionally, for the server-side code that requires shared access across multiple EC2 instances, Amazon FSx for Windows File Server should be used. FSx for Windows File Server provides a high-performance file system that is compatible with Windows Server workloads and can be mounted on each EC2 instance.

解析：To ensure high availability of the storage solution for the gaming application, the solutions architect should store the static files on Amazon S3 and use Amazon CloudFront to cache objects at the edge, which will help in distributing the content globally and reducing latency. Additionally, for the server-side code that requires shared access across multiple EC2 instances, Amazon FSx for Windows File Server should be used. FSx for Windows File Server provides a high-performance file system that is compatible with Windows Server workloads and can be mounted on each EC2 instance.

44. Question #362A 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.)

- 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.

答案：BE

解析：To ensure that messages are received in the same order they were sent, especially when dealing with a payment ID as a unique identifier, the solutions architect should write the messages to an Amazon SQS FIFO queue. By setting the message group to use the payment ID, the SQS FIFO queue ensures that messages with the same payment ID are processed in the order they were sent. Additionally, writing the messages to an Amazon DynamoDB table with the payment ID as the partition key can provide a mechanism to store and retrieve messages reliably, although this option alone does not guarantee order. However, when combined with SQS FIFO, it can serve as a secondary storage mechanism for the messages.

解析：To ensure that messages are received in the same order they were sent, especially when dealing with a payment ID as a unique identifier, the solutions architect should write the messages to an Amazon SQS FIFO queue. By setting the message group to use the payment ID, the SQS FIFO queue ensures that messages with the same payment ID are processed in the order they were sent. Additionally, writing the messages to an Amazon DynamoDB table with the payment ID as the partition key can provide a mechanism to store and retrieve messages reliably, although this option

alone does not guarantee order. However, when combined with SQS FIFO, it can serve as a secondary storage mechanism for the messages.

45. Question #364A 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.)

- 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.

答案：BD

解析：To ensure that data is encrypted at rest and in transit, and only accessible to authorized personnel, the solutions architect should enable server-side encryption on the SQS components using an AWS KMS customer managed key (Option D) and apply a key policy to restrict key usage to authorized principals. Additionally, enabling server-side encryption on the SNS components with a customer managed key (Option B) and applying a key policy for access control will ensure that messages published and subscribed to are also encrypted and secure. Setting a condition in the

queue policy to allow only encrypted connections over TLS further secures the data in transit.

解析: To ensure that data is encrypted at rest and in transit, and only accessible to authorized personnel, the solutions architect should enable server-side encryption on the SQS components using an AWS KMS customer managed key (Option D) and apply a key policy to restrict key usage to authorized principals. Additionally, enabling server-side encryption on the SNS components with a customer managed key (Option B) and applying a key policy for access control will ensure that messages published and subscribed to are also encrypted and secure. Setting a condition in the queue policy to allow only encrypted connections over TLS further secures the data in transit.

46. Question #371A 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.)

- 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.

答案: CD

解析: To meet the requirement with the least operational overhead, the solutions architect should enable EBS encryption by default in the AWS Region where the EKS cluster will be created and select the customer managed key as the default key (Option C). This ensures that all EBS volumes created in the region are automatically encrypted with the specified key. Additionally, creating an IAM role with a policy that grants permission to use the customer managed key and associating the role with the EKS cluster (Option D) ensures that the cluster has the necessary permissions to encrypt and decrypt data at rest using the key.

解析: To meet the requirement with the least operational overhead, the solutions architect should enable EBS encryption by default in the AWS Region where the EKS cluster will be created and select the customer managed key as the default key (Option C). This ensures that all EBS volumes created in the region are automatically encrypted with the specified key. Additionally, creating an IAM role with a policy that grants permission to use the customer managed key and associating the role with the EKS cluster (Option D) ensures that the cluster has the necessary permissions to encrypt and decrypt data at rest using the key.

47. Question #387A 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.)

- 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.

答案：DE

解析：To follow the principle of least privilege, the solutions architect should create a new IAM user for the deployment engineer and assign permissions that are specific to the tasks they need to perform. This can be accomplished by either creating an IAM policy that allows only AWS CloudFormation actions (Option D) or by creating an IAM role with explicit permissions for CloudFormation and having the deployment engineer use that role when launching stacks (Option E). Both options provide a level of access that is scoped to the necessary actions for deploying resources with CloudFormation, without granting broader or unnecessary permissions.

解析：To follow the principle of least privilege, the solutions architect should create a new IAM user for the deployment engineer and assign permissions that are specific to the tasks they need to perform. This can be accomplished by either creating an IAM policy that allows only AWS CloudFormation actions (Option D) or by creating an IAM role with explicit permissions for CloudFormation and having the deployment engineer use that role when launching stacks (Option E). Both options provide a level of access that is scoped to the necessary actions for deploying resources with CloudFormation, without granting broader or unnecessary permissions.

48. Question #390A 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.)

- 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.

答案：BD

解析：Based on the company's requirements for optimizing customer session management during transactions in their three-tier ecommerce application, two solutions that will meet these requirements are: 1. Use an Amazon DynamoDB table to store customer session information. 2. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.

Here's why these solutions are appropriate:

- 1. Amazon DynamoDB:
 - DynamoDB is a fully managed NoSQL database that provides fast and predictable performance with seamless scalability.
 - It offers durable storage for session data, meeting the requirement for storing session data durably.
 - DynamoDB can handle high-concurrency workloads, making it suitable for ecommerce applications with potentially high traffic.
 - It integrates well with other AWS services and can be easily accessed from EC2 instances.
- 2. Amazon ElastiCache for Redis:
 - ElastiCache for Redis is an in-memory data store that provides sub-millisecond latency, making it excellent for session management.
 - Redis supports data persistence, ensuring that session data is stored durably.
 - It offers high availability with Multi-AZ deployments and automatic failover.
 - ElastiCache for Redis is highly scalable and can handle large volumes of session data.
 - Both solutions allow the application to store session data externally from the EC2 instances, which is crucial when running instances in an Auto Scaling group. This approach ensures that session data remains accessible even if individual instances are terminated or new ones are launched.
 - When implementing either of these solutions, consider the following best practices:
 - Implement proper encryption for data at rest and in transit to protect customer session information.
 - Use IAM roles and policies to manage access to DynamoDB or ElastiCache, following the principle of least privilege.
 - Configure appropriate TTL (Time to Live) for session data to automatically expire old sessions.
 -

Monitor and set up alarms for performance metrics to ensure optimal operation. – Regularly backup your session data, especially if using DynamoDB. Remember to test your chosen solution thoroughly in a non-production environment before deploying to production. Also, consult the AWS documentation for the most up-to-date information on implementing these services for session management in your ecommerce application.

Sources [1] [Valkey-, Memcached-, and Redis OSS-Compatible Cache – Amazon ElastiCache with Valkey- and Redis OSS-compatibility – AWS] (<https://aws.amazon.com/elasticsearch/redis/>) [3] [Amazon ElastiCache and Self-Managed Redis – Database Caching Strategies Using Redis] (<https://docs.aws.amazon.com/whitepapers/latest/database-caching-strategies-using-redis/amazon-elasticsearch-and-self-managed-redis.html>) [6] [Amazon ElastiCache (Redis OSS) – Architecting for HIPAA Security and Compliance on Amazon Web Services] (<https://docs.aws.amazon.com/whitepapers/latest/architecting-hipaa-security-and-compliance-on-aws/amazon-elasticsearch-for-redis.html>)

解析: Based on the company's requirements for optimizing customer session management during transactions in their three-tier ecommerce application, two solutions that will meet these requirements are: 1. Use an Amazon DynamoDB table to store customer session information. 2. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.

Here's why these solutions are appropriate: 1. Amazon DynamoDB: – DynamoDB is a fully managed NoSQL database that provides fast and predictable performance with seamless scalability. – It offers durable storage for session data, meeting the requirement for storing session data durably. – DynamoDB can handle high-concurrency workloads, making it suitable for ecommerce applications with potentially high traffic.

– It integrates well with other AWS services and can be easily accessed from EC2 instances. 2. Amazon ElastiCache for Redis: – ElastiCache for Redis is an in-memory data store that provides sub-millisecond latency, making it excellent for session management. – Redis supports data persistence, ensuring that session data is stored durably. – It offers high availability with Multi-AZ deployments and automatic failover. – ElastiCache for Redis is highly scalable and can handle large volumes of

session data. Both solutions allow the application to store session data externally from the EC2 instances, which is crucial when running instances in an Auto Scaling group. This approach ensures that session data remains accessible even if individual instances are terminated or new ones are launched. When implementing either of these solutions, consider the following best practices:

- Implement proper encryption for data at rest and in transit to protect customer session information.
- Use IAM roles and policies to manage access to DynamoDB or ElastiCache, following the principle of least privilege.
- Configure appropriate TTL (Time to Live) for session data to automatically expire old sessions.
- Monitor and set up alarms for performance metrics to ensure optimal operation.
- Regularly backup your session data, especially if using DynamoDB. Remember to test your chosen solution thoroughly in a non-production environment before deploying to production. Also, consult the AWS documentation for the most up-to-date information on implementing these services for session management in your ecommerce application.

Sources [1] [Valkey-, Memcached-, and Redis OSS-Compatible Cache – Amazon ElastiCache with Valkey- and Redis OSS-compatibility – AWS] (<https://aws.amazon.com/elasticsearch/redis/>) [3] [Amazon ElastiCache and Self-Managed Redis – Database Caching Strategies Using Redis] (<https://docs.aws.amazon.com/whitepapers/latest/database-caching-strategies-using-redis/amazon-elasticsearch-and-self-managed-redis.html>) [6] [Amazon ElastiCache (Redis OSS) – Architecting for HIPAA Security and Compliance on Amazon Web Services] (<https://docs.aws.amazon.com/whitepapers/latest/architecting-hipaa-security-and-compliance-on-aws/amazon-elasticsearch-for-redis.html>)

49. Question #405A 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?

- 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.

答案：DE

解析：D: A target tracking scaling policy is ideal for dynamically scaling the Auto Scaling group based on real-time metrics such as CPU utilization, ensuring the system meets traffic demand during peak hours. E: Scheduled scaling allows the Auto Scaling group to reduce capacity to zero during weekends and revert to default values at the start of the workweek, optimizing cost while meeting demand.

解析：D: A target tracking scaling policy is ideal for dynamically scaling the Auto Scaling group based on real-time metrics such as CPU utilization, ensuring the system meets traffic demand during peak hours. E: Scheduled scaling allows the Auto Scaling group to reduce capacity to zero during weekends and revert to default values at the start of the workweek, optimizing cost while meeting demand.

50. Question #406A 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?
- 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.

答案：CD

解析：To meet the requirements, the solutions architect should create a security group for the web servers in the public subnet (Option C) and configure it to allow traffic from anywhere on port 443, as the web servers must be open to the internet. Additionally, a security group for the DB instance (Option D) should be created with a rule that allows traffic only from the security group associated with the web servers on port 3306. This ensures that only the web servers can access the DB instance on the required port, while the DB instance is not exposed to the public internet.

解析：To meet the requirements, the solutions architect should create a security group for the web servers in the public subnet (Option C) and configure it to allow traffic from anywhere on port 443, as the web servers must be open to the internet. Additionally, a security group for the DB instance (Option D) should be created with a rule that allows traffic only from the security group associated with the web servers on port 3306. This ensures that only the web servers can access the DB instance on the required port, while the DB instance is not exposed to the public internet.

51. Question #416A 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.)
- 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.

答案：BD

解析：To resolve the issue of slow page loads, the solutions architect should set up an Amazon CloudFront distribution (Option B) to cache static and dynamic content closer to users, reducing latency.

Additionally, creating a read replica for the RDS DB instance (Option D) can help offload read queries from the primary database, improving the performance of the web application.

解析：To resolve the issue of slow page loads, the solutions architect should set up an Amazon CloudFront distribution (Option B) to cache static and dynamic content closer to users, reducing latency.

Additionally, creating a read replica for the RDS DB instance (Option D) can help offload read queries from the primary database, improving the performance of the web application.

52. Question #419A 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.)

- 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.

答案：CE

解析：To enforce the use of encrypted EBS volumes with minimal impact on employees, the company should create a service control policy (SCP) that denies the creation of unencrypted EBS volumes (Option C) and specify a default EBS volume encryption setting in the Organizations management account (Option E). The SCP will automatically apply the necessary restrictions, and the default encryption setting will ensure that all new volumes are created with encryption by default.

解析：To enforce the use of encrypted EBS volumes with minimal impact on employees, the company should create a service control policy (SCP) that denies the creation of unencrypted EBS volumes (Option C) and specify a default EBS volume encryption setting in the Organizations management account (Option E). The SCP will automatically apply the necessary restrictions, and the default encryption setting will ensure that all new volumes are created with encryption by default.

53. Question #423A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions: Which IAM principals can the solutions architect attach this policy to? (Choose two.)

```
{    "Statement": [
        {
            "Action": [
                "ssm>ListDocuments",
                "ssm>GetDocument"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Sid": ""
        }
    ],
    "Version": "2012-10-17"
}
```

- A. Role
- B. Group
- C. Organization
- D. Amazon Elastic Container Service (Amazon ECS) resource
- E. Amazon EC2 resource

答案：AB

解析：An identity-based policy in AWS is attached to an identity, which can be an IAM user, group, or role. Therefore, options A (Role) and B (Group) are correct. Options C (Organization), D (Amazon ECS resource), and E (Amazon EC2 resource) are not IAM principals to which policies are directly attached. Instead, they may be associated with policies through other means, such as resource-based policies or service control policies (SCPs).

解析：An identity-based policy in AWS is attached to an identity, which can be an IAM user, group, or role. Therefore, options A (Role) and B (Group) are correct. Options C (Organization), D (Amazon ECS resource), and E (Amazon EC2 resource) are not IAM principals to which policies are directly attached. Instead, they may be associated with policies through other means, such as resource-based policies or service control policies (SCPs).

54. Question #430A 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.)

- 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.

答案：BC

解析：Option B is cost-effective because AWS Lambda functions can be triggered by S3 events, such as the upload of a new .csv file, and can convert the file into an image without the need for a running EC2 instance. Option C is also cost-effective as it manages the lifecycle of the files; .csv files can be transitioned to a cheaper storage class after one day, and image files that are no longer needed after 30 days can be expired, thus saving on storage costs.

解析：Option B is cost-effective because AWS Lambda functions can be triggered by S3 events, such as the upload of a new .csv file, and can convert the file into an image without the need for a running EC2 instance. Option C is also cost-effective as it manages the lifecycle of the files; .csv files can be transitioned to a cheaper storage class after one day, and image files that are no longer needed after 30 days

can be expired, thus saving on storage costs.

55. Question #440A 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.)

- 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.

答案：AC

解析：Option A is correct because Amazon Aurora can restore from a snapshot taken from an RDS instance for the same database engine. Option C is also correct because mysqldump is a common utility for exporting MySQL databases, and the resulting dump file can be imported directly into Aurora. Options B, D, and E are not necessary since they involve additional steps that are not required for the process.

解析：Option A is correct because Amazon Aurora can restore from a snapshot taken from an RDS instance for the same database engine. Option C is also correct because mysqldump is a common utility for exporting MySQL databases, and the resulting dump file can be imported directly into Aurora. Options B, D, and E are not necessary since they involve additional steps that are not required for the process.

56. Question #450A 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.)

- 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.

答案: CEF

解析: Option C is correct as it suggests refactoring the application to follow best practices by separating the tiers and hosting them in different subnets, which enhances security and scalability. Option E is also correct as it involves using Elastic Load Balancers to distribute traffic and increase the availability of the web tier. Option F is correct because it recommends using a Multi-AZ RDS deployment for the

database tier, which provides high availability and fault tolerance.

解析: Option C is correct as it suggests refactoring the application to follow best practices by separating the tiers and hosting them in different subnets, which enhances security and scalability. Option E is also correct as it involves using Elastic Load Balancers to distribute traffic and increase the availability of the web tier. Option F is correct because it recommends using a Multi-AZ RDS deployment for the database tier, which provides high availability and fault tolerance.

57. Question #451A 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.)

- 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

答案: BCF

解析: Option B is correct as the operational team will be responsible for creating RDS instances and scheduling maintenance windows. Option C is correct because configuring additional software components for monitoring and management is a task for the operational team when using ECS. Option F is correct as the encryption of data in transit is a concern that the operational team would manage, especially with Direct Connect establishing a private network connection.

解析: Option B is correct as the operational team will be responsible for creating RDS instances and scheduling maintenance windows. Option C is correct because configuring additional software components for monitoring and management is a task for the operational team when using ECS. Option F is correct as the encryption of data in transit is a concern that the operational team would manage, especially with Direct Connect establishing a private network connection.

58. Question #455A 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.)

- 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 configuration 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.

答案: BDF

解析: Option B is correct as AWS Budgets can be used to create budgets and set the budget amounts directly from the Billing dashboards. Option D is correct because creating an IAM role for AWS Budgets allows for the

necessary permissions to manage budget actions. Option F is correct as it enables the company to receive alerts when the budget threshold is met and to take action, such as preventing the provisioning of additional resources, through an IAM identity with an appropriate SCP.

解析: Option B is correct as AWS Budgets can be used to create budgets and set the budget amounts directly from the Billing dashboards. Option D is correct because creating an IAM role for AWS Budgets allows for the necessary permissions to manage budget actions. Option F is correct as it enables the company to receive alerts when the budget threshold is met and to take action, such as preventing the provisioning of additional resources, through an IAM identity with an appropriate SCP.

59. Question #458A solutions architect is designing a RESTAPI 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.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon RDS
- D. Amazon DynamoDB

答案: BC

解析: Option B, AWS Lambda, is a serverless compute service that can handle the execution of code with the required memory allocation without the need for managing servers. Option C, Amazon RDS, is a relational database service that can provide the necessary relational data storage. Using these two services together would meet the requirements with minimal administrative effort, as they are both managed services that abstract away much of the infrastructure management.

解析: Option B, AWS Lambda, is a serverless compute service that can handle the execution of code with the required memory allocation without the need for managing servers. Option C, Amazon RDS, is a relational database service that can provide the necessary relational data storage.

Using these two services together would meet the requirements with minimal administrative effort, as they are both managed services that abstract away much of the infrastructure management.

60. Question #484A 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.)
- 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.

答案：AE

解析：Option A involves creating a new organization in AWS Organizations, which is necessary for consolidating multiple AWS accounts under a single management structure. Option E involves setting up AWS IAM Identity Center and integrating it with the company's corporate directory service, which allows for centralized authentication across all AWS accounts in the organization.

解析：Option A involves creating a new organization in AWS Organizations, which is necessary for consolidating multiple AWS accounts under a single management structure. Option E involves setting up AWS IAM Identity Center and integrating it with the company's corporate directory service,

which allows for centralized authentication across all AWS accounts in the organization.

61. Question #493A 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.)

- 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.

答案：DEF

解析：The correct combination of steps is D, E, and F. First, use Amazon Transcribe (D) to convert the audio recordings into text in their original languages. Then, use Amazon Translate (E) to translate the transcribed text into English. Finally, use Amazon Comprehend (F) to analyze the English text and create sentiment analysis reports.

解析：The correct combination of steps is D, E, and F. First, use Amazon Transcribe (D) to convert the audio recordings into text in their original languages. Then, use Amazon Translate (E) to translate the transcribed text into English. Finally, use Amazon Comprehend (F) to analyze the English text and create sentiment analysis reports.

62. Question #496A 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.)

- 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.

答案：BD

解析：Option B, deploying an AWS Storage Gateway file gateway, can replace the NFS storage and provide access to NFS shares over the network. Option D, deploying an AWS Storage Gateway volume gateway, can replace block storage and provide high-performance block-level storage for on-premises applications. Both solutions support local caching and do not require re-architecting existing applications.

解析：Option B, deploying an AWS Storage Gateway file gateway, can replace the NFS storage and provide access to NFS shares over the network. Option D, deploying an AWS Storage Gateway volume gateway, can replace block storage and provide high-performance block-level storage for on-premises applications. Both solutions support local caching and do not require re-architecting existing applications.

63. Question #500A 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.)

- 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.

答案：AD

解析：Option A is correct because AWS DataSync can be used to transfer data from on-premises file servers directly to Amazon FSx for Windows File Server, and it can preserve file permissions during the migration. Option D is also correct as it involves using AWS Snowcone, which can be connected to the on-premises network and used in conjunction with DataSync to facilitate the transfer of data to the new file system.

解析：Option A is correct because AWS DataSync can be used to transfer data from on-premises file servers directly to Amazon FSx for Windows File Server, and it can preserve file permissions during the migration. Option D is also correct as it involves using AWS Snowcone, which can be connected to the on-premises network and used in conjunction with DataSync to facilitate the transfer of data to the new file system.

64. Question #502A 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.

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.

答案：CE

解析：Option C is correct because Amazon EFS provides a scalable and resilient file storage system that can be mounted on multiple EC2 instances, which improves the resilience of the website's image storage. Option E is also correct as it involves setting up an Auto Scaling group with an Application Load Balancer and using Amazon CloudFront, which can improve the performance and resilience of the website by distributing content closer to users worldwide.

解析：Option C is correct because Amazon EFS provides a scalable and resilient file storage system that can be mounted on multiple EC2 instances, which improves the resilience of the website's image storage. Option E is also correct as it involves setting up an Auto Scaling group with an Application Load Balancer and using Amazon CloudFront, which can improve the performance and resilience of the website by distributing content closer to users worldwide.

65. Question #508A 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 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 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 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.

答案：BD

解析：Option B and D are the solutions that meet the requirements with the least administrative effort. By using AWS Backup, the company can automate the backup process for EC2 instances. Option B allows for the creation of an AMI lifecycle policy that automates the backup process and configures the copy to the us-west-2 Region. Option D further simplifies the process by using AWS Backup to define the destination for the backup copy in us-west-2 and schedules the backup to run twice daily, ensuring

that data loss does not exceed 24 hours.

解析: Option B and D are the solutions that meet the requirements with the least administrative effort. By using AWS Backup, the company can automate the backup process for EC2 instances. Option B allows for the creation of an AMI lifecycle policy that automates the backup process and configures the copy to the us-west-2 Region. Option D further simplifies the process by using AWS Backup to define the destination for the backup copy in us-west-2 and schedules the backup to run twice daily, ensuring that data loss does not exceed 24 hours.

66. Question #515A 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.)
- 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

答案: BCE

解析: Option B is correct as Amazon Redshift supports encryption for data at rest and in transit. Option C is suitable because Amazon Redshift is designed for analytics workloads, which can be scheduled to run during off-peak hours. Option E is correct as Amazon Redshift can scale to handle large amounts of data and high request volumes, making it suitable for global data warehousing needs.

解析: Option B is correct as Amazon Redshift supports encryption for data at rest and in transit. Option C is suitable because Amazon Redshift is designed for analytics workloads, which can be scheduled to run during off-peak hours. Option E is correct as Amazon Redshift can scale to

handle large amounts of data and high request volumes, making it suitable for global data warehousing needs.

67. Question #522A 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.)
- 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.

答案：BC

解析：Options B and C are correct because they provide automated scaling solutions that require minimal manual intervention. The Kubernetes Metrics Server (option B) provides the metrics that are necessary for the Kubernetes Cluster Autoscaler (option C) to make informed decisions about scaling the cluster up or down based on the current workload. This combination allows the EKS cluster to scale efficiently in response to varying demand without the need for manual adjustments or additional services.

解析：Options B and C are correct because they provide automated scaling solutions that require minimal manual intervention. The Kubernetes Metrics Server (option B) provides the metrics that are necessary for the Kubernetes Cluster Autoscaler (option C) to make informed decisions about scaling the cluster up or down based on the current workload. This combination allows the EKS cluster to scale efficiently in response to varying demand without the need for manual adjustments or additional services.

68. Question #532A 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.)

- 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).

答案：ADF

解析：Option A is necessary to create a wildcard domain that can apply to all customers. Option D is required to secure the custom domain with a wildcard certificate, ensuring HTTPS connections for all customers without the need to manage individual certificates. Option F is needed to set up a custom domain name in API Gateway and link it with the ACM certificate for secure access. Options B, C, and E are not required as they either add unnecessary complexity or do not contribute to the operational efficiency of providing individual and secure URLs.

解析：Option A is necessary to create a wildcard domain that can apply to all customers. Option D is required to secure the custom domain with a wildcard certificate, ensuring HTTPS connections for all customers without the need to manage individual certificates. Option F is needed to set up a custom domain name in API Gateway and link it with the ACM certificate for secure access. Options B, C, and E are not required as they either add unnecessary complexity or do not contribute to the

operational efficiency of providing individual and secure URLs.

69. Question #541A 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.)
- 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.

答案：ACE

解析：Option A is correct as AWS Lambda can handle unpredictable workloads efficiently, scaling down when not in use to save costs. Option C is necessary for user authentication, ensuring only paying customers can access the application. Option E is cost-effective for serving web content, as AWS Amplify can automate the deployment of static assets and CloudFront can cache and distribute content globally to reduce latency. Option B is less cost-effective due to the ongoing operational costs associated with managing an ECS service and ALB. Option D is not needed as identity pools are used for providing temporary AWS credentials to access AWS services, which is not required for this scenario. Option F is less efficient because it involves managing PHP scripts on S3, which is not designed to run server-side code.

解析: Option A is correct as AWS Lambda can handle unpredictable workloads efficiently, scaling down when not in use to save costs. Option C is necessary for user authentication, ensuring only paying customers can access the application. Option E is cost-effective for serving web content, as AWS Amplify can automate the deployment of static assets and CloudFront can cache and distribute content globally to reduce latency. Option B is less cost-effective due to the ongoing operational costs associated with managing an ECS service and ALB. Option D is not needed as identity pools are used for providing temporary AWS credentials to access AWS services, which is not required for this scenario. Option F is less efficient because it involves managing PHP scripts on S3, which is not designed to run server-side code.

70. Question #543A 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.)

- 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.

答案: AD

解析: To use Savings Plan discounts across multiple AWS accounts, you'll need to set up consolidated billing using AWS Organizations. Here's how to accomplish this task:

1. Create an AWS Organization – Log in to the AWS account that has the existing EC2 instances and Savings Plan.
 - Navigate to the AWS Organizations console.
 - Click "Create organization" and follow the prompts to set up the organization.This account will become the management account for the organization.
2. Invite Other AWS Accounts – In the AWS Organizations console of the management account, go to the "Accounts" tab.
 - Click "Add account" and choose "Invite existing account".
 - Enter the account ID or email address for each AWS account you want to invite.
 - Send the invitations.
3. Accept Invitations in Member Accounts – Log in to each invited AWS account.
 - Go to the AWS Organizations console.
 - Find and accept the invitation to join the organization.
4. Enable Discount Sharing – Log in to the management account.
 - Go to the AWS Account Management console.
 - Navigate to the billing preferences section.
 - Turn on discount sharing for the organization.
5. Verify Consolidated Billing – In the management account, go to the AWS Billing console.
 - Confirm that you can see billing information for all member accounts.
 - Verify that Savings Plan discounts are being applied across accounts.By completing these steps, you've set up consolidated billing through AWS Organizations and enabled Savings Plan discount sharing across your accounts. This allows you to maximize the benefits of your Savings Plan even after decommissioning some EC2 instances. Remember to regularly review your Savings Plan utilization and adjust as needed to optimize cost savings across your organization. Also, consider implementing additional cost management practices, such as using AWS Cost Explorer and setting up AWS Budgets, to maintain visibility and control over your AWS spending across all accounts.

Sources [1] [Consolidating billing for AWS Organizations – AWS Billing] (<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>) [3] [Setting up Scenario 3: Separate AWS account for each user – Setting Up Multi-User Environments in AWS (for Classroom Training and Research)] (<https://docs.aws.amazon.com/whitepapers/latest/setting-up-multi-user-environments/setting-up-scenario-3-separate-aws-account-for-each-user-setting-up-multi-user-environments.html>)

ing-up-scenario-3-separate-aws-account-for-each-user.html) [6] [Multiple organizations – Organizing Your AWS Environment Using Multiple Accounts] (<https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/multiple-organizations.html>)

解析: To use Savings Plan discounts across multiple AWS accounts, you'll need to set up consolidated billing using AWS Organizations. Here's how to accomplish this task:

1. Create an AWS Organization – Log in to the AWS account that has the existing EC2 instances and Savings Plan. – Navigate to the AWS Organizations console. – Click "Create organization" and follow the prompts to set up the organization. – This account will become the management account for the organization.
2. Invite Other AWS Accounts – In the AWS Organizations console of the management account, go to the "Accounts" tab. – Click "Add account" and choose "Invite existing account". – Enter the account ID or email address for each AWS account you want to invite. – Send the invitations.
3. Accept Invitations in Member Accounts – Log in to each invited AWS account. – Go to the AWS Organizations console. – Find and accept the invitation to join the organization.
4. Enable Discount Sharing – Log in to the management account. – Go to the AWS Account Management console. – Navigate to the billing preferences section.
 - Turn on discount sharing for the organization.
5. Verify Consolidated Billing – In the management account, go to the AWS Billing console.
 - Confirm that you can see billing information for all member accounts.
 - Verify that Savings Plan discounts are being applied across accounts. By completing these steps, you've set up consolidated billing through AWS Organizations and enabled Savings Plan discount sharing across your accounts. This allows you to maximize the benefits of your Savings Plan even after decommissioning some EC2 instances. Remember to regularly review your Savings Plan utilization and adjust as needed to optimize cost savings across your organization. Also, consider implementing additional cost management practices, such as using AWS Cost Explorer and setting up AWS Budgets, to maintain visibility and control over your AWS spending across all accounts.

Sources [1] [Consolidating billing for AWS Organizations – AWS Billing] (<https://docs.aws.amazon.com>)

[/awsaccountbilling/latest/aboutv2/consolidated-billing.html](https://awsaccountbilling/latest/aboutv2/consolidated-billing.html)) [3] [Setting up Scenario 3: Separate AWS account for each user – Setting Up Multi-User Environments in AWS (for Classroom Training and Research)] (<https://docs.aws.amazon.com/whitepapers/latest/setting-up-multi-user-environments/setting-up-scenario-3-separate-aws-account-for-each-user.html>) [6] [Multiple organizations – Organizing Your AWS Environment Using Multiple Accounts] (<https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/multiple-organizations.html>)

71. Question #550A 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.)

- 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.

答案：BD

解析：The correct steps are B and D. The Lambda execution role must have permissions to use the AWS KMS key for decryption, which is accomplished by adding the necessary permissions (kms:Decrypt and kms:GenerateDataKey) to the execution role's policy (Option B). Additionally, the AWS KMS key policy must be updated to allow the Lambda execution role to perform these actions on the key (Option D). The Lambda resource policy (Option A) and the Lambda function policy (Option C) are not the correct locations to grant these permissions. The execution role is the appropriate entity to receive permissions for accessing KMS keys.

解析：The correct steps are B and D. The Lambda execution role must have permissions to use the AWS KMS key for decryption, which is accomplished by adding the necessary permissions (kms:Decrypt and kms:GenerateDataKey) to the execution role's policy (Option B). Additionally, the AWS KMS key policy must be updated to allow the Lambda execution role to perform

these actions on the key (Option D). The Lambda resource policy (Option A) and the Lambda function policy (Option C) are not the correct locations to grant these permissions. The execution role is the appropriate entity to receive permissions for accessing KMS keys.

72. Question #559A company hosts multiple applications on AWS for different product lines. The applications use different compute resources, including Amazon EC2 instances and Application Load Balancers. The applications run in different AWS 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.)
- 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.

答案：BE

解析：To utilize the consolidated billing feature in AWS Organizations for detailed cost analysis, the company should select a specific user-defined tag in the AWS Billing console (Option B) that is consistently applied across all accounts to categorize costs by product line. Additionally, activating the selected tag from the Organizations management account (Option E) ensures that the tagging policy is applied across all accounts within the organization, enabling accurate cost allocation and reporting.

解析：To utilize the consolidated billing feature in AWS Organizations for detailed cost analysis, the company should select a specific user-defined tag in the AWS Billing console (Option B) that is consistently applied across all accounts to categorize costs by product line. Additionally, activating the selected tag from the Organizations management account (Option E) ensures that the tagging policy is applied

across all accounts within the organization, enabling accurate cost allocation and reporting.

73. Question #562A 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.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create an interface VPC 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.

答案：AB

解析：To ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet, the solutions architect should take the following combination of steps: 1. Create a gateway endpoint for DynamoDB. 2. Create a route table entry for the endpoint. Here's a more detailed explanation of these steps and their benefits: 1. Create a gateway endpoint for DynamoDB:

- This allows EC2 instances in the VPC to communicate with DynamoDB using private IP addresses.
- Traffic between the VPC and DynamoDB stays within the AWS network, never traversing the public internet.
- This improves security by reducing exposure to potential internet-based threats.

2. Create a route table entry for the endpoint:

- After creating the gateway endpoint, AWS automatically adds a route to the selected route tables.
- This route directs traffic destined for DynamoDB to the gateway endpoint.
- Ensures that traffic from EC2 instances to DynamoDB uses the private endpoint instead of the internet gateway.

By implementing these steps, the solutions architect can meet the requirement of keeping API calls between EC2 instances and DynamoDB within the AWS network, enhancing security and potentially improving performance. Best practices and additional considerations:

- Use IAM

policies to control access to DynamoDB through the VPC endpoint. – Regularly review and update the endpoint policies to maintain the principle of least privilege. – Consider using VPC flow logs to monitor traffic patterns and ensure that DynamoDB traffic is indeed using the gateway endpoint. – Ensure that security groups and network ACLs are properly configured to allow the necessary traffic between EC2 instances and the DynamoDB endpoint. – Periodically review and test the setup to ensure it continues to meet security and performance requirements.

Remember to consult the AWS documentation for the most up-to-date information on configuring and managing VPC endpoints for DynamoDB.

Sources [1] [Infrastructure security in Amazon DynamoDB – Amazon DynamoDB] (<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/network-isolation.html>) [3] [Securing DynamoDB connections using VPC endpoints and IAM policies” – Amazon DynamoDB] (<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/inter-network-traffic-privacy.html>) [6] [Gateway endpoints for Amazon DynamoDB – Amazon Virtual Private Cloud] (<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>)

解析: To ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet, the solutions architect should take the following combination of steps: 1. Create a gateway endpoint for DynamoDB. 2. Create a route table entry for the endpoint. Here's a more detailed explanation of these steps and their benefits: 1. Create a gateway endpoint for DynamoDB: – This allows EC2 instances in the VPC to communicate with DynamoDB using private IP addresses. – Traffic between the VPC and DynamoDB stays within the AWS network, never traversing the public internet. – This improves security by reducing exposure to potential internet-based threats. 2. Create a route table entry for the endpoint: – After creating the gateway endpoint, AWS automatically adds a route to the selected route tables. – This route directs traffic destined for DynamoDB to the gateway endpoint. – Ensures that traffic from EC2 instances to DynamoDB uses the private endpoint instead of the internet gateway. By implementing these steps, the solutions architect can meet the

requirement of keeping API calls between EC2 instances and DynamoDB within the AWS network, enhancing security and potentially improving performance. Best practices and additional considerations:

- Use IAM policies to control access to DynamoDB through the VPC endpoint.
- Regularly review and update the endpoint policies to maintain the principle of least privilege.
- Consider using VPC flow logs to monitor traffic patterns and ensure that DynamoDB traffic is indeed using the gateway endpoint.
- Ensure that security groups and network ACLs are properly configured to allow the necessary traffic between EC2 instances and the DynamoDB endpoint.
- Periodically review and test the setup to ensure it continues to meet security and performance requirements.

Remember to consult the AWS documentation for the most up-to-date information on configuring and managing VPC endpoints for DynamoDB.

Sources [1] [Infrastructure security in Amazon DynamoDB – Amazon DynamoDB] (<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/network-isolation.html>) [3] [Securing DynamoDB connections using VPC endpoints and IAM policies” – Amazon DynamoDB] (<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/inter-network-traffic-privacy.html>) [6] [Gateway endpoints for Amazon DynamoDB – Amazon Virtual Private Cloud] (<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>)

74. Question #598A 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.)

- 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.

答案：ACF

解析：The combination of deploying an AWS Storage Gateway on premises in Amazon S3 File Gateway mode (Option A), setting up an AWS Glue crawler to create a table based on the data in Amazon S3 (Option C), and setting up Amazon Athena to query the data in Amazon S3 (Option F) is the most cost-effective solution. This setup allows for seamless data transfer from on-premises SMB shares to Amazon S3, automated table creation for easier data discovery, and serverless, pay-per-query analytics with Athena for analysts to run SQL commands. This avoids the need for a dedicated EMR cluster (Option D) or Redshift cluster (Option E), which would incur higher costs and management overhead.

解析：The combination of deploying an AWS Storage Gateway on premises in Amazon S3 File Gateway mode (Option A), setting up an AWS Glue crawler to create a table based on the data in Amazon S3 (Option C), and setting up Amazon Athena to query the data in Amazon S3 (Option F) is the most cost-effective solution. This setup allows for seamless data transfer from on-premises SMB shares to Amazon S3, automated table creation for easier data discovery, and serverless, pay-per-query analytics with Athena for analysts to run SQL commands. This avoids the need for a dedicated EMR cluster (Option D) or Redshift cluster (Option E), which would incur higher costs and management overhead.

75. Question #599A 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.)

- 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

答案：ACE

解析：The operational team is responsible for providing resilient power and network connectivity to the Outposts racks (Option A), ensuring the physical security and access controls of the data center environment (Option C), and the physical maintenance of Outposts components (Option E). These responsibilities align with the company's need to support the infrastructure requirements of AWS Outposts within their on-premises data center. Managing the virtualization hypervisor and AWS services (Option B) is typically an AWS responsibility when using Outposts, while ensuring the availability of the Outposts infrastructure (Option D) is also an AWS responsibility. Providing extra capacity for ECS clusters (Option F) would be a concern for the team managing the application's scalability rather than the operational team focused on the data center environment.

解析：The operational team is responsible for providing resilient power and network connectivity to the Outposts racks (Option A), ensuring the physical security and access controls of the data center environment (Option C), and the physical maintenance of Outposts components (Option E). These responsibilities align with the company's need to support the infrastructure requirements of AWS Outposts within their on-premises data center. Managing the virtualization hypervisor and AWS services (Option

B) is typically an AWS responsibility when using Outposts, while ensuring the availability of the Outposts infrastructure (Option D) is also an AWS responsibility. Providing extra capacity for ECS clusters (Option F) would be a concern for the team managing the application's scalability rather than the operational team focused on the data center environment.

76. Question #617A 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.)

- 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.

答案：BE

解析：The combination of Option B, creating an Amazon EFS file system, and Option E, installing an AWS DataSync agent for migration, is the most cost-effective solution. Amazon EFS is a scalable NFS file system that can be accessed by multiple AWS resources, making it suitable for the requirement of multiple resources accessing the data. DataSync provides an efficient and automated way to migrate data from on-premises storage to AWS without disrupting existing services. Option A, Amazon FSx for Lustre, is not the best choice as it is designed for high-performance computing (HPC) workloads and may be overprovisioned for the given data size. Option C, using Amazon S3, does not meet the NFS protocol requirement. Option D, manually copying data, is not cost-effective and could lead to service interruption.

解析: The combination of Option B, creating an Amazon EFS file system, and Option E, installing an AWS DataSync agent for migration, is the most cost-effective solution. Amazon EFS is a scalable NFS file system that can be accessed by multiple AWS resources, making it suitable for the requirement of multiple resources accessing the data. DataSync provides an efficient and automated way to migrate data from on-premises storage to AWS without disrupting existing services. Option A, Amazon FSx for Lustre, is not the best choice as it is designed for high-performance computing (HPC) workloads and may be overprovisioned for the given data size. Option C, using Amazon S3, does not meet the NFS protocol requirement. Option D, manually copying data, is not cost-effective and could lead to service interruption.

77. Question #622A 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.)

- 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.

答案：CD

解析: Option C, deploying Amazon DynamoDB with auto scaling enabled, and Option D, deploying static content into an Amazon S3 bucket with a CloudFront distribution, are the solutions that provide the most scalability. DynamoDB auto scaling adjusts the capacity automatically to maintain performance as the workload changes, allowing for rapid schema evolution and handling the varying number of users. S3 combined with CloudFront provides a highly scalable and cost-effective solution for serving static content with low latency across the globe. Option A, provisioning on-demand capacity, does not provide the scalability of auto scaling. Option B, using Aurora serverless, may not scale as quickly to handle the morning peak as DynamoDB can. Option E, deploying EC2 instances with EFS, would not be as scalable or cost-effective for serving static content compared to using S3 and CloudFront.

解析: Option C, deploying Amazon DynamoDB with auto scaling enabled, and Option D, deploying static content into an Amazon S3 bucket with a CloudFront distribution, are the solutions that provide the most scalability. DynamoDB auto scaling adjusts the capacity automatically to maintain performance as the workload changes, allowing for rapid schema evolution and handling the varying number of users. S3 combined with CloudFront provides a highly scalable and cost-effective solution for serving static content with low latency across the globe. Option A, provisioning on-demand capacity, does not provide the scalability of auto scaling. Option B, using Aurora serverless, may not scale as quickly to handle the morning peak as DynamoDB can. Option E, deploying EC2 instances with EFS, would not be as scalable or cost-effective for serving static content compared to using S3 and CloudFront.

78. Question #637A 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.)

- A. AWS Fargate
- B. AWS Lambda
- C. AWS DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

答案：BC

解析：Option B, AWS Lambda, and Option C, AWS DynamoDB, are the services that meet the requirements. AWS Lambda can handle unpredictable request patterns by scaling automatically from a few requests to hundreds of thousands of requests per second. DynamoDB is a key-value and document database that can store and query data with low latency, making it suitable for the less than 1 GB of data that needs to be persisted. The combination of Lambda and DynamoDB provides a serverless architecture that can scale quickly to handle the workload without the need for manual intervention.

解析：Option B, AWS Lambda, and Option C, AWS DynamoDB, are the services that meet the requirements. AWS Lambda can handle unpredictable request patterns by scaling automatically from a few requests to hundreds of thousands of requests per second. DynamoDB is a key-value and document database that can store and query data with low latency, making it suitable for the less than 1 GB of data that needs to be persisted. The combination of Lambda and DynamoDB provides a serverless architecture that can scale quickly to handle the workload without the need for manual intervention.

79. Question #640A 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.)

- 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.

答案：BE

解析：To ensure the Lambda function can decrypt files from Amazon S3, the Lambda function's execution role must have the necessary permissions to use the KMS key for decryption. This is achieved by granting the decrypt permission to the Lambda IAM role in the KMS key's policy (Option B). Additionally, an IAM policy with the kms:decrypt permission should be created and attached to the Lambda function (Option D). Option A is incorrect because it does not specify the attachment to the execution role. Option C is incorrect because it suggests granting permissions to the Lambda resource policy, which is not the correct practice. Option E is partially correct but redundant since the execution role already implies the necessary permissions for the Lambda function.

解析：To ensure the Lambda function can decrypt files from Amazon S3, the Lambda function's execution role must have the necessary permissions to use the KMS key for decryption. This is achieved by granting the decrypt permission to the Lambda IAM role in the KMS key's policy (Option B). Additionally, an IAM policy with the kms:decrypt permission should be created and attached to the Lambda function (Option D). Option A is incorrect because it does not specify the attachment to the execution role. Option C is incorrect because it suggests granting permissions to the Lambda resource policy, which is not the correct practice. Option E is partially correct but redundant since the execution role already implies the necessary permissions for the Lambda function.

80. Question #644An 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.)

- A. Use the 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 the 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 the 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 to the DNS provider.
- E. Validate domain ownership for the domain by adding the required DNS records to the DNS provider.

答案：AE

解析：To encrypt website data in transit, the company needs to use SSL/TLS certificates. Option A involves requesting a public certificate for the apex domain and a wildcard certificate for all subdomains from AWS Certificate Manager, which is necessary for SSL/TLS encryption. Option E is about validating domain ownership using DNS records, which is a preferred method for ensuring that the certificate is issued correctly for the domain. Option B is incorrect because private certificates are not suitable for public-facing websites, and Option C is not necessary since a single public certificate can cover both the apex and subdomains. Option D is not required as DNS validation (Option E) is the preferred method.

解析：To encrypt website data in transit, the company needs to use SSL/TLS certificates. Option A involves requesting a public certificate for the apex domain and a wildcard certificate for all subdomains from AWS Certificate Manager, which is necessary for SSL/TLS encryption. Option E is about validating domain ownership using DNS records, which is a preferred method for ensuring that the certificate is issued correctly

for the domain. Option B is incorrect because private certificates are not suitable for public-facing websites, and Option C is not necessary since a single public certificate can cover both the apex and subdomains. Option D is not required as DNS validation (Option E) is the preferred method.

81. Question #655A 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.)

- 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.

答案：CE

解析：To achieve session affinity and apply a WAF for additional security, the company should create a public Application Load Balancer (ALB) and specify the application target group, which is option C. The ALB supports sticky sessions, ensuring a better user experience. Additionally, creating a web ACL in AWS WAF and associating it with the ALB endpoint, as in option E, will provide the necessary security for the application's internet-facing endpoint.

解析：To achieve session affinity and apply a WAF for additional security, the company should create a public Application Load Balancer (ALB) and specify the application target group, which is option C. The ALB supports sticky sessions, ensuring a better user experience.

Additionally, creating a web ACL in AWS WAF and associating it with the ALB endpoint, as in option E, will provide the necessary security for the application's internet-facing endpoint.

82. Question #658A 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.)

- A. Deploy compute optimized EC2 instances into a cluster placement group.
- B. Deploy compute optimized EC2 instances into a partition placement group.
- C. Launch an Amazon FSx for Lustre file system.
- D. Launch an Amazon FSx for OpenZFS file system.
- E. Launch an Amazon FSx for NetApp ONTAP file system.

答案: AE

解析: To achieve the lowest latency for HPC workloads that require multi-protocol access (NFS and SMB), the company should deploy compute optimized EC2 instances into a cluster placement group (Option A), which is designed to provide low-latency and high-throughput network connectivity between instances. Additionally, launching an Amazon FSx for NetApp ONTAP file system (Option E) will meet the requirements as it supports both NFS and SMB protocols, and is designed to offer high performance for file-sharing workloads.

解析: To achieve the lowest latency for HPC workloads that require multi-protocol access (NFS and SMB), the company should deploy compute optimized EC2 instances into a cluster placement group (Option A), which is designed to provide low-latency and high-throughput network connectivity between instances. Additionally, launching an Amazon FSx for NetApp ONTAP file system (Option E) will meet the requirements as it supports both NFS and SMB protocols, and is designed to offer high performance for file-sharing workloads.

83. Question #666A 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.)

- 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.

答案：BE

解析：To achieve high availability without modifying the application code, the architect should migrate the MySQL database to an Amazon RDS for MySQL Multi-AZ DB instance (Option B), which automatically provides failover and redundancy within the AWS infrastructure. Additionally, creating an Application Load Balancer (Option E) to distribute traffic to an Auto Scaling group of EC2 instances across two Availability Zones ensures that the application layer is also highly available. These two actions together provide a highly available architecture for the web application.

解析：To achieve high availability without modifying the application code, the architect should migrate the MySQL database to an Amazon RDS for MySQL Multi-AZ DB instance (Option B), which automatically provides failover and redundancy within the AWS infrastructure. Additionally, creating an Application Load Balancer (Option E) to distribute traffic to an Auto Scaling group of EC2 instances across two Availability Zones

ensures that the application layer is also highly available. These two actions together provide a highly available architecture for the web application.

84. Question #674A 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.)

- 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.

答案：BD

解析：To resolve the performance issues, the solutions architect should create a read replica for the DB instance (Option B) and configure the application to send read traffic to the read replica. This will help distribute the read load and improve the overall performance of the database during high-traffic periods. Additionally, creating an Amazon ElastiCache cluster (Option D) and configuring the application to cache query results can further enhance performance by reducing the number of database queries, especially for frequently accessed data.

解析：To resolve the performance issues, the solutions architect should create a read replica for the DB instance (Option B) and configure the application to send read traffic to the read replica. This will help distribute the read load and improve the overall performance of the

database during high-traffic periods. Additionally, creating an Amazon ElastiCache cluster (Option D) and configuring the application to cache query results can further enhance performance by reducing the number of database queries, especially for frequently accessed data.

85. Question #679A 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.)

- 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.

答案：ACE

解析：To meet the requirements, the company should create an S3 bucket with S3 Object Lock enabled (Option A) to prevent the backups from being deleted or overwritten for a specified retention period. Configuring a default retention period of 30 days (Option C) ensures that the backups will be retained for the required duration. Finally, setting up an S3 Lifecycle policy to expire the objects after 30 days (Option E) automates the deletion process after the retention period ends, ensuring that the backups are automatically removed from S3 after 30 days.

解析：To meet the requirements, the company should create an S3 bucket with S3 Object Lock enabled (Option A) to prevent the backups from being deleted or overwritten for a specified retention period. Configuring a default retention period of 30 days (Option C) ensures that the backups will be retained for the required duration. Finally, setting up an S3 Lifecycle policy to expire the objects after 30 days (Option E) automates the deletion process after the retention period ends, ensuring that the

backups are automatically removed from S3 after 30 days.

86. Question #683A 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.)

- 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.

答案：AC

解析：To improve application resiliency with minimal changes, the company should migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (Option A), which ensures high availability and fault tolerance for the web tier. Additionally, migrating the database to an Amazon RDS Multi-AZ deployment (Option C) provides a managed, highly available database solution with automatic failover, which improves resiliency without the need to manage the underlying infrastructure.

解析：To improve application resiliency with minimal changes, the company should migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (Option A), which ensures high availability and fault tolerance for the web tier. Additionally, migrating the database to an Amazon RDS Multi-AZ deployment (Option C) provides a managed, highly available database solution with automatic failover, which improves resiliency without the need to manage the underlying infrastructure.

87. #Question #687A 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.)

- 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.

答案：DE

解析：Since the company has no ML experience and is looking for a managed service, Amazon Forecast is a fully managed service that can be used to create predictors based on historical data without the need for training a model manually (Option E). Additionally, to automate and trigger the prediction process, a Lambda function can be configured to use the Amazon Forecast predictor, which aligns with Option D. Options A, B, and C are not the most suitable as they involve either manual training of models or do not leverage the managed service that Amazon Forecast provides.

解析：Since the company has no ML experience and is looking for a managed service, Amazon Forecast is a fully managed service that can be used to create predictors based on historical data without the need for training a model manually (Option E). Additionally, to automate and trigger the prediction process, a Lambda function can be configured to use the Amazon Forecast predictor, which aligns with Option D. Options A, B, and C are not the most suitable as they involve either manual training of models or do not leverage the managed service that Amazon Forecast provides.

88. #Question #690A 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.)

- 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.

答案：CD

解析：To scale throughput for both uploading to Amazon S3 and downloading to EC2 instances, the company can use S3 multipart uploads (Option C), which allows for the parallel uploading of parts of a file, thus increasing throughput. Additionally, fetching multiple byte-ranges of an object in parallel (Option D) can increase download throughput by allowing the EC2 instances to download different parts of the file simultaneously. Using S3 access points (Option A) or uploading into multiple S3 buckets (Option B) may offer other benefits but do not directly contribute to scaling throughput. Adding a random prefix to each object (Option E) would not affect throughput.

解析：To scale throughput for both uploading to Amazon S3 and downloading to EC2 instances, the company can use S3 multipart uploads (Option C), which allows for the parallel uploading of parts of a file, thus increasing throughput. Additionally, fetching multiple byte-ranges of an object in parallel (Option D) can increase download throughput by allowing the EC2 instances to download different parts of the file simultaneously. Using S3 access points (Option A) or uploading into multiple S3 buckets (Option B) may offer other benefits but do not directly contribute to scaling throughput. Adding a random prefix to each object (Option E) would not affect throughput.

89. #Question #691A 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.)

- 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 no-cache. Use Amazon CloudFront to deliver the content.

答案：BE

解析：To ensure strong consistency for a web application with frequent content changes, the architect should use Amazon EFS (Option B), which provides a shared file system that can be mounted on multiple EC2 instances across Availability Zones and maintains strong consistency. Additionally, using Amazon S3 with Amazon CloudFront (Option E) can provide a scalable and highly available solution for web content delivery, with CloudFront automatically updating its cache when new content is published to the S3 bucket.

解析：To ensure strong consistency for a web application with frequent content changes, the architect should use Amazon EFS (Option B), which provides a shared file system that can be mounted on multiple EC2 instances across Availability Zones and maintains strong consistency. Additionally, using Amazon S3 with Amazon CloudFront (Option E) can

provide a scalable and highly available solution for web content delivery, with CloudFront automatically updating its cache when new content is published to the S3 bucket.

90. #Question #700A 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.)

- 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.

答案：BC

解析：Based on the requirements for the gaming company's new internet-facing application, I recommend the following combination of actions:

- 1. Create external Application Load Balancers (ALBs) in front of the application in each Region.
- 2. Create an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region.

Here's why these actions are recommended:

- 1. External Application Load Balancers (ALBs):
 - ALBs are designed for internet-facing applications and support both TCP and UDP protocols.
 - They provide high availability within each region by distributing traffic across multiple Availability Zones.
 - ALBs offer advanced routing and security features suitable for gaming applications.
- 2. AWS Global Accelerator:
 - Global Accelerator improves availability and performance for applications with a global user base.
 - It uses Anycast IP addresses to route traffic to

the nearest AWS edge location, reducing latency for global users. – Global Accelerator automatically routes traffic to the healthiest regional endpoints, ensuring high availability. – It works seamlessly with Application Load Balancers, making it an ideal choice for this scenario. By combining these two solutions, the gaming company can achieve:

- High availability through multi-region deployment and intelligent traffic routing
- Minimum latency for global users by leveraging AWS's global network and edge locations
- Support for both TCP and UDP protocols required by the application
- Improved resilience against regional failures or network issues

Best practices to consider:

- Implement proper health checks for the ALBs to ensure traffic is only routed to healthy instances.
- Use AWS Shield Standard (included with Global Accelerator) for DDoS protection.
- Consider implementing AWS WAF with the ALBs for additional layer 7 protection.
- Regularly monitor and optimize the application's performance using AWS CloudWatch and Global Accelerator's telemetry.

For the most up-to-date information on Global Accelerator features, pricing, and best practices, please refer to the official AWS documentation. Sources

- [1] [Multi-Region and hybrid architecture for low-latency games – Games Industry Lens] (<https://docs.aws.amazon.com/wellarchitected/latest/games-industry-lens/games-scenario-1.4.html>)
- [3] [Resilience in AWS Global Accelerator – AWS Global Accelerator] (<https://docs.aws.amazon.com/global-accelerator/latest/dg/disaster-recovery-resiliency.html>)
- [6] [Modernize game backend services with AWS Global Accelerator | AWS for Games Blog] (<https://aws.amazon.com/blogs/gametech/modernize-game-backend-services-with-aws-global-accelerator/>)

解析: Based on the requirements for the gaming company's new internet-facing application, I recommend the following combination of actions:

1. Create external Application Load Balancers (ALBs) in front of the application in each Region.
2. Create an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region.

Here's why these actions are recommended:

- 1. External Application Load Balancers (ALBs):
 - ALBs are designed for internet-facing applications and support both TCP and UDP protocols.
 - They provide high availability

within each region by distributing traffic across multiple Availability Zones.

- ALBs offer advanced routing and security features suitable for gaming applications.

2. AWS Global Accelerator:

- Global Accelerator improves availability and performance for applications with a global user base.
- It uses Anycast IP addresses to route traffic to the nearest AWS edge location, reducing latency for global users.
- Global Accelerator automatically routes traffic to the healthiest regional endpoints, ensuring high availability.
- It works seamlessly with Application Load Balancers, making it an ideal choice for this scenario.
- By combining these two solutions, the gaming company can achieve:

 - High availability through multi-region deployment and intelligent traffic routing
 - Minimum latency for global users by leveraging AWS's global network and edge locations
 - Support for both TCP and UDP protocols required by the application
 - Improved resilience against regional failures or network issues

Best practices to consider:

 - Implement proper health checks for the ALBs to ensure traffic is only routed to healthy instances.
 - Use AWS Shield Standard (included with Global Accelerator) for DDoS protection.
 - Consider implementing AWS WAF with the ALBs for additional layer 7 protection.
 - Regularly monitor and optimize the application's performance using AWS CloudWatch and Global Accelerator's telemetry.

For the most up-to-date information on Global Accelerator features, pricing, and best practices, please refer to the official AWS documentation.

Sources

 - [1] [Multi-Region and hybrid architecture for low-latency games – Games Industry Lens] (<https://docs.aws.amazon.com/wellarchitected/latest/games-industry-lens/games-scenario-1.4.html>)
 - [3] [Resilience in AWS Global Accelerator – AWS Global Accelerator] (<https://docs.aws.amazon.com/global-accelerator/latest/dg/disaster-recovery-resiliency.html>)
 - [6] [Modernize game backend services with AWS Global Accelerator | AWS for Games Blog] (<https://aws.amazon.com/blogs/gametech/modernize-game-backend-services-with-aws-global-accelerator/>)

91. #Question #705A 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.)

- 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.

答案：AD

解析：To replicate data changes during the migration from an RDS MySQL instance to an Aurora PostgreSQL cluster, the company should use AWS DMS with change data capture (CDC) (Option D). This feature allows for the continuous replication of changes made to the source database.

Additionally, AWS DMS Schema Conversion (Option A) can be used to transform the database schema from MySQL to PostgreSQL, ensuring compatibility between the two different database systems. Creating a read replica on the RDS MySQL instance (Option B) or configuring an Aurora MySQL read replica (Option C) does not directly address the replication of data changes during the migration process. Promoting a read replica to a standalone cluster (Option E) is part of the migration process but does not by itself replicate data changes.

解析：To replicate data changes during the migration from an RDS MySQL instance to an Aurora PostgreSQL cluster, the company should use AWS DMS with change data capture (CDC) (Option D). This feature allows for the continuous replication of changes made to the source database.

Additionally, AWS DMS Schema Conversion (Option A) can be used to transform the database schema from MySQL to PostgreSQL, ensuring

compatibility between the two different database systems. Creating a read replica on the RDS MySQL instance (Option B) or configuring an Aurora MySQL read replica (Option C) does not directly address the replication of data changes during the migration process. Promoting a read replica to a standalone cluster (Option E) is part of the migration process but does not by itself replicate data changes.

92. #Question #709A 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.)

- 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.

答案：BE

解析：To apply the SCP that restricts the launch of EC2 instances of certain sizes in nonproduction accounts, the most effective solutions are to attach the SCP directly to the nonproduction member accounts (Option B) and to create a separate OU for the nonproduction accounts, then attach the SCP to that OU (Option E). Attaching the SCP to the root OU (Option A) would apply the policy to all accounts, including the production account, which is not the intention. Attaching the SCP to the management account (Option C) or creating an OU for the production account (Option D) would not effectively target the nonproduction accounts as required.

解析: To apply the SCP that restricts the launch of EC2 instances of certain sizes in nonproduction accounts, the most effective solutions are to attach the SCP directly to the nonproduction member accounts (Option B) and to create a separate OU for the nonproduction accounts, then attach the SCP to that OU (Option E). Attaching the SCP to the root OU (Option A) would apply the policy to all accounts, including the production account, which is not the intention. Attaching the SCP to the management account (Option C) or creating an OU for the production account (Option D) would not effectively target the nonproduction accounts as required.

93. #Question #737A 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.)

- 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.

答案：CE

解析：To keep replication in SYNC across all three regions, we use Bi-directional Multi-Region Access Point for video streaming and uploads. → uploads to nearest Low latency region and Bi-directional replication will keep other two regions in SYNC this reducing the upload and streaming latency.

解析：To keep replication in SYNC across all three regions, we use Bi-directional Multi-Region Access Point for video streaming and uploads. → uploads to nearest Low latency region and Bi-directional replication will keep other two regions in SYNC this reducing the upload and streaming latency.

94. #Question #746A 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.)

- 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.

答案：AC

解析：To achieve the lowest possible latency for processing streaming data in near-real time on Amazon EC2 instances, the solutions architect should enable and configure enhanced networking (Option A) on each EC2 instance, which can significantly reduce network latency. Additionally, running the EC2 instances in a cluster placement group (Option C) can help to reduce latency by ensuring that instances are placed close together in the same Availability Zone. Grouping instances in separate accounts (Option B) would not contribute to lower latency and could increase complexity. Attaching multiple elastic network interfaces (Option D) is typically used for increasing network bandwidth, not

latency reduction. Using EBS-optimized instance types (Option E) improves the performance of EBS volumes but does not affect network latency.

解析: To achieve the lowest possible latency for processing streaming data in near-real time on Amazon EC2 instances, the solutions architect should enable and configure enhanced networking (Option A) on each EC2 instance, which can significantly reduce network latency. Additionally, running the EC2 instances in a cluster placement group (Option C) can help to reduce latency by ensuring that instances are placed close together in the same Availability Zone. Grouping instances in separate accounts (Option B) would not contribute to lower latency and could increase complexity. Attaching multiple elastic network interfaces (Option D) is typically used for increasing network bandwidth, not latency reduction. Using EBS-optimized instance types (Option E) improves the performance of EBS volumes but does not affect network latency.

95. #Question #752A 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.)

- 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.

答案: AD

解析: To meet the requirements of minimal infrastructure management and exactly-once delivery for application messaging, the solutions architect

should use AWS Lambda (Option A) for the compute layers, which is a serverless compute service that requires no infrastructure management.

解析: To meet the requirements of minimal infrastructure management and exactly-once delivery for application messaging, the solutions architect should use AWS Lambda (Option A) for the compute layers, which is a serverless compute service that requires no infrastructure management.

96. #Question #772A 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.)

- 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.

答案: AB

解析: Based on the requirements provided in the question, the two solutions that best meet the company's needs are: 1. A. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate 2. B. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate Here's why these solutions are the most appropriate: 1. Managed service: Both Amazon ECS and Amazon EKS are fully managed container orchestration services, which aligns with the company's desire to use a managed service to host their Docker container-based application. 2. Scalability: AWS Fargate, when used with either ECS or EKS, provides automatic scaling of individual container services based on demand. This meets the requirement for appropriate scaling in and out. 3. Minimal operational overhead: By using

AWS Fargate with either ECS or EKS, the company eliminates the need to manage the underlying infrastructure. Fargate removes the need to provision, configure, or scale clusters of virtual machines, thus meeting the requirement of not adding operational overhead or infrastructure to manage.

4. Flexibility: Both solutions offer the flexibility to run containerized applications without the complexity of managing the underlying compute resources. These solutions allow the company to focus on developing and running their applications rather than managing the infrastructure. They provide the benefits of containerization along with the ease of use and scalability of managed AWS services. The other options do not fully meet the stated requirements:

- Option C (API Gateway with Lambda) is not designed for running Docker containers directly.
- Options D and E (ECS or EKS with EC2 worker nodes) would require managing the underlying EC2 instances, which adds operational overhead and doesn't align with the requirement of no additional infrastructure to manage.

For the most up-to-date information on these services and their capabilities, I recommend referring to the official AWS documentation. Sources [1] [Amazon Elastic Container Service – Overview of Deployment Options on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/overview-deployment-options/amazon-elastic-container-service.html>) [3] [Containers services on AWS – Containers on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/containers-on-aws/containers-services-on-aws.html>) [6] [Containers on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/containers-on-aws/index.html>)

解析: Based on the requirements provided in the question, the two solutions that best meet the company's needs are:

1. A. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate
2. B. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate

Here's why these solutions are the most appropriate:

1. Managed service: Both Amazon ECS and Amazon EKS are fully managed container orchestration services, which aligns with the company's desire to use a managed service to host their Docker container-based application.
2. Scalability: AWS Fargate, when used with either ECS or EKS, provides automatic scaling of individual container services based on demand. This meets the requirement for

appropriate scaling in and out.

3. Minimal operational overhead: By using AWS Fargate with either ECS or EKS, the company eliminates the need to manage the underlying infrastructure. Fargate removes the need to provision, configure, or scale clusters of virtual machines, thus meeting the requirement of not adding operational overhead or infrastructure to manage.

4. Flexibility: Both solutions offer the flexibility to run containerized applications without the complexity of managing the underlying compute resources. These solutions allow the company to focus on developing and running their applications rather than managing the infrastructure. They provide the benefits of containerization along with the ease of use and scalability of managed AWS services. The other options do not fully meet the stated requirements:

- Option C (API Gateway with Lambda) is not designed for running Docker containers directly.
- Options D and E (ECS or EKS with EC2 worker nodes) would require managing the underlying EC2 instances, which adds operational overhead and doesn't align with the requirement of no additional infrastructure to manage.

For the most up-to-date information on these services and their capabilities, I recommend referring to the official AWS documentation. Sources

- [1] [Amazon Elastic Container Service – Overview of Deployment Options on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/overview-deployment-options/amazon-elastic-container-service.html>)
- [3] [Containers services on AWS – Containers on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/containers-on-aws/containers-services-on-aws.html>)
- [6] [Containers on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/containers-on-aws/index.html>)

97. #Question #777A 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.)
- 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.

答案：AC

解析：To allow the development organizational unit (OU) to access and launch AMIs that are encrypted with AWS KMS keys, the solutions architect should add the development team's OU ARN to the launch permission list for the AMIs (Option A) and update the key policy to allow the development team's OU to use the AWS KMS keys that are used to decrypt the snapshots (Option C). These steps ensure that the development team has the necessary permissions to access and use the AMIs while maintaining the security and encryption of the underlying snapshots.

解析：To allow the development organizational unit (OU) to access and launch AMIs that are encrypted with AWS KMS keys, the solutions architect should add the development team's OU ARN to the launch permission list for the AMIs (Option A) and update the key policy to allow the development team's OU to use the AWS KMS keys that are used to decrypt the snapshots (Option C). These steps ensure that the development team has the necessary permissions to access and use the AMIs while maintaining the security and encryption of the underlying snapshots.

98. #Question #790A 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.)

- 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.

答案：BE

解析：To provide high availability and scalability for the web application without rewriting it, the solutions architect should configure Amazon EC2 Auto Scaling with multiple Availability Zones in private subnets (Option B) and configure an Application Load Balancer in a public subnet to distribute web traffic (Option E). Auto Scaling can ensure that multiple instances of the application are running in different Availability Zones, providing fault tolerance and handling increased load. The Application Load Balancer can distribute incoming traffic across these instances, ensuring that user demand is met without overloading a single instance.

解析：To provide high availability and scalability for the web application without rewriting it, the solutions architect should configure Amazon EC2 Auto Scaling with multiple Availability Zones in private subnets (Option B) and configure an Application Load Balancer in a public subnet to distribute web traffic (Option E). Auto Scaling can ensure that multiple instances of the application are running in different Availability Zones, providing fault tolerance and handling increased load. The Application Load Balancer can distribute incoming traffic across these instances, ensuring that user demand is met without overloading a single instance.

99. #Question #795A 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.)

- 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.

答案：BD

解析：To optimize a high performance computing (HPC) environment in AWS for networking and storage, the solutions architect should create an Amazon FSx for Lustre file system (Option B) and attach an Elastic Fabric Adapter (EFA) to the Amazon EC2 instances (Option D). Amazon FSx for Lustre is a high-performance file system that provides the high-throughput and low-latency access required for HPC workloads. Configuring it with scratch storage can improve performance by storing temporary data locally. Additionally, EFA enables high-throughput and low-latency networking for HPC applications by providing a scalable and high-performance network interface for EC2 instances.

解析：To optimize a high performance computing (HPC) environment in AWS for networking and storage, the solutions architect should create an Amazon FSx for Lustre file system (Option B) and attach an Elastic Fabric Adapter (EFA) to the Amazon EC2 instances (Option D). Amazon FSx for Lustre is a high-performance file system that provides the high-throughput and low-latency access required for HPC workloads. Configuring it with scratch storage can improve performance by storing temporary data locally. Additionally, EFA enables high-throughput and low-latency networking for HPC applications by providing a scalable and high-performance network interface for EC2 instances.

100. Question #859A 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.)

- 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.

答案：AC

解析：To optimize costs, the finance team should review Trusted Advisor recommendations for Reserved Instance Optimization and Idle DB Instances. These checks can provide insights into potential savings by optimizing the use of RDS instances.

解析：To optimize costs, the finance team should review Trusted Advisor recommendations for Reserved Instance Optimization and Idle DB Instances. These checks can provide insights into potential savings by optimizing the use of RDS instances.

101. Question #865A 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.)

- 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.

答案：AE

解析：Based on the company's requirements for a scalable and serverless solution to enhance the performance of their near-real-time streaming application, I recommend the following combination of steps:

1. Use Amazon Kinesis Data Firehose to ingest the data.
2. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Here's why these options are recommended:

- 1. Amazon Kinesis Data Firehose:
 - It's a fully managed, serverless service for ingesting streaming data.
 - Scales automatically to match the throughput of your data.
 - Can handle large amounts of incoming data efficiently.
 - Integrates seamlessly with other AWS services for data processing and storage.
- 2. AWS Fargate with Amazon ECS:
 - Provides a serverless compute engine for containers.
 - Allows you to run long-running tasks (up to 30 minutes or more) without managing the underlying infrastructure.
 - Scales automatically based on the defined task requirements.
 - Offers more flexibility for complex processing jobs compared to AWS Lambda, which has a maximum execution time limit.

This combination addresses the key requirements:

- Scalability: Both services scale automatically to handle varying loads.
- Serverless: No need to manage underlying infrastructure.
- Performance enhancement: By using managed services designed for high-throughput data processing. Additionally, this solution allows for better cost optimization as you only pay for the resources you use during data processing.

To implement this solution:

1. Set up a Kinesis Data Firehose delivery stream to ingest the streaming data.
2. Create container images with your data processing logic.
3. Define ECS tasks using these container images.
4. Configure Fargate to run these ECS tasks as the data comes in through Firehose.

Remember to monitor the performance using Amazon CloudWatch and adjust the configuration as needed to optimize for your specific workload.

Sources [1] [Streaming architecture patterns using a modern data architecture – Build Modern Data Streaming Architectures on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/build-modern-data-streaming-analytics-architectures/streaming-analytics-architecture-patterns-using-a-modern-data-architecture.html>)

[3] [Scenario 2: Near-real-time data for security teams – Streaming Data

Solutions on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/streaming-data-solutions-amazon-kinesis/scenario-2.html>) [6] [Streaming processing – Serverless Applications Lens] (<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/streaming-processing.html>)

解析: Based on the company's requirements for a scalable and serverless solution to enhance the performance of their near-real-time streaming application, I recommend the following combination of steps: 1. Use Amazon Kinesis Data Firehose to ingest the data. 2. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data. Here's why these options are recommended: 1. Amazon Kinesis Data Firehose: – It's a fully managed, serverless service for ingesting streaming data. – Scales automatically to match the throughput of your data. – Can handle large amounts of incoming data efficiently. – Integrates seamlessly with other AWS services for data processing and storage. 2. AWS Fargate with Amazon ECS: – Provides a serverless compute engine for containers. – Allows you to run long-running tasks (up to 30 minutes or more) without managing the underlying infrastructure. – Scales automatically based on the defined task requirements. – Offers more flexibility for complex processing jobs compared to AWS Lambda, which has a maximum execution time limit. This combination addresses the key requirements: – Scalability: Both services scale automatically to handle varying loads. – Serverless: No need to manage underlying infrastructure. – Performance enhancement: By using managed services designed for high-throughput data processing. Additionally, this solution allows for better cost optimization as you only pay for the resources you use during data processing. To implement this solution: 1. Set up a Kinesis Data Firehose delivery stream to ingest the streaming data. 2. Create container images with your data processing logic. 3. Define ECS tasks using these container images. 4. Configure Fargate to run these ECS tasks as the data comes in through Firehose. Remember to monitor the performance using Amazon CloudWatch and adjust the configuration as needed to optimize for your specific workload. Sources [1] [Streaming architecture patterns using a modern data architecture – Build Modern

Data Streaming Architectures on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/build-modern-data-streaming-analytics-architectures/streaming-analytics-architecture-patterns-using-a-modern-data-architecture.html>) [3] [Scenario 2: Near-real-time data for security teams – Streaming Data Solutions on AWS] (<https://docs.aws.amazon.com/whitepapers/latest/streaming-data-solutions-amazon-kinesis/scenario-2.html>) [6] [Streaming processing – Serverless Applications Lens] (<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/streaming-processing.html>)

102. Question #866A 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?

- 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 VPC. Create 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.

答案：A

解析：A gateway VPC endpoint for Amazon S3 allows the VPC to privately access S3, ensuring that sensitive data does not traverse the public internet. This is achieved by routing traffic directly to S3 through the AWS network.

解析：A gateway VPC endpoint for Amazon S3 allows the VPC to privately access S3, ensuring that sensitive data does not traverse the public internet. This is achieved by routing traffic directly to S3 through the AWS network.

103. Question #876A 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.)

- 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.

答案：BD

解析：To achieve high availability cost-effectively, a Network Load Balancer (NLB) can distribute traffic at the transport layer (layer 4) to EC2 instances. Additionally, creating an Auto Scaling group that spans multiple Availability Zones ensures that the application remains available even if one zone experiences an outage.

解析：To achieve high availability cost-effectively, a Network Load Balancer (NLB) can distribute traffic at the transport layer (layer 4) to EC2 instances. Additionally, creating an Auto Scaling group that spans multiple Availability Zones ensures that the application remains available even if one zone experiences an outage.

104. Question #879A company runs an e-commerce 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.)

- 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 RESTAPI with a usage plan.

答案：BC

解析：Based on the e-commerce application's scalability issues and the need for a cost-effective solution to meet peak usage demands, I recommend the following combination of actions:

1. 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.
2. Configure the application to use an Amazon ElastiCache cluster in front of the Aurora PostgreSQL DB cluster.

Here's why these actions are the most cost-effective and efficient solutions:

- 1. Using Amazon SQS with Auto Scaling:
 - This decouples the purchase processing from the main application, allowing for better scalability.
 - SQS acts as a buffer during peak times, preventing application timeouts.
 - Auto Scaling ensures that EC2 instances are added or removed based on the queue length, optimizing costs.
 - This approach handles traffic spikes efficiently without overprovisioning resources.
- 2. Implementing Amazon ElastiCache:
 - ElastiCache can significantly reduce the load on the Aurora PostgreSQL DB cluster by caching frequently accessed data.
 - This improves response times for common queries, reducing the likelihood of timeouts.
 - It's a cost-effective way to scale read performance without upgrading the database instance.

These solutions address both the application and database layers, providing a comprehensive approach to handling peak usage. They allow the system to scale dynamically based on demand while optimizing costs. Additional best

practices to consider:

- Implement proper monitoring and alerting using Amazon CloudWatch to track performance metrics and trigger scaling actions.
- Regularly review and optimize your database queries to ensure efficient use of resources.
- Consider using read replicas for Aurora PostgreSQL to distribute read traffic if read-heavy operations are causing bottlenecks. Remember to thoroughly test these changes in a non-production environment before implementing them in your live system.

Also, consult the AWS documentation for the most up-to-date information on service limits and best practices for your specific use case. Sources

- [1] [AWS Auto Scaling FAQs] (<https://aws.amazon.com/autoscaling/faqs/>)
- [3] [Hyperscaling Aurora MySQL-Compatible to handle sudden traffic growth
- AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/hyper-scale-aurora-mysql/introduction.html>)
- [6] [Community | EC2 cost optimization:15 ways to save on Amazon EC2] (<https://community.aws/content/2hQNGTh6vpw0HTgKELzL8mkqmKb/ec2-cost-optimization-15-ways-to-save-on-amazon-ec2>)

解析: Based on the e-commerce application's scalability issues and the need for a cost-effective solution to meet peak usage demands, I recommend the following combination of actions:

1. 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.
2. Configure the application to use an Amazon ElastiCache cluster in front of the Aurora PostgreSQL DB cluster. Here's why these actions are the most cost-effective and efficient solutions:

- 1. Using Amazon SQS with Auto Scaling:
 - This decouples the purchase processing from the main application, allowing for better scalability.
 - SQS acts as a buffer during peak times, preventing application timeouts.
 - Auto Scaling ensures that EC2 instances are added or removed based on the queue length, optimizing costs.
 - This approach handles traffic spikes efficiently without overprovisioning resources.
- 2. Implementing Amazon ElastiCache:
 - ElastiCache can significantly reduce the load on the Aurora PostgreSQL DB cluster by caching frequently accessed data.
 - This improves response times for common queries, reducing the likelihood of timeouts.
 - It's a cost-effective way to

scale read performance without upgrading the database instance. These solutions address both the application and database layers, providing a comprehensive approach to handling peak usage. They allow the system to scale dynamically based on demand while optimizing costs. Additional best practices to consider:

- Implement proper monitoring and alerting using Amazon CloudWatch to track performance metrics and trigger scaling actions.
- Regularly review and optimize your database queries to ensure efficient use of resources.
- Consider using read replicas for Aurora PostgreSQL to distribute read traffic if read-heavy operations are causing bottlenecks. Remember to thoroughly test these changes in a non-production environment before implementing them in your live system.

Also, consult the AWS documentation for the most up-to-date information on service limits and best practices for your specific use case. Sources

- [1] [AWS Auto Scaling FAQs] (<https://aws.amazon.com/autoscaling/faqs/>)
- [3] [Hyperscaling Aurora MySQL-Compatible to handle sudden traffic growth – AWS Prescriptive Guidance] (<https://docs.aws.amazon.com/prescriptive-guidance/latest/hyper-scale-aurora-mysql/introduction.html>)
- [6] [Community | EC2 cost optimization:15 ways to save on Amazon EC2] (<https://community.aws/content/2hQNGTh6vpw0HTgKELzL8mkqmKb/ec2-cost-optimization-15-ways-to-save-on-amazon-ec2>)

105. Question #881A 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.)

- 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.

答案：AC

解析：Setting a Cache-Control private directive on S3 objects ensures that the content is cached for a single user and is not served stale to other users. Setting the CloudFront default TTL to 2 minutes provides a short caching period, which, when combined with the Cache-Control directive, allows for quick invalidation of content after updates.

解析：Setting a Cache-Control private directive on S3 objects ensures that the content is cached for a single user and is not served stale to other users. Setting the CloudFront default TTL to 2 minutes provides a short caching period, which, when combined with the Cache-Control directive, allows for quick invalidation of content after updates.

106. Question#233A 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.)

- 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.

答案：AB

107. Question #884A 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.)

- 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.

答案：ACE

解析：Correct Answer Combination and Explanation: A. Configure the security group for the web tier to allow inbound HTTPS traffic from the security group for the ALB. – Correct. The web tier needs to receive incoming HTTPS traffic from the ALB, which is the entry point for users over the internet. C. Configure the security group for the database tier to allow inbound Microsoft SQL Server traffic from the security group for the application tier. – Correct. The database tier should only accept traffic from the application tier, which contains the business logic that requires access to the database. E. Configure the security group for the application tier to allow inbound HTTPS traffic from the security group for the web tier. – Correct. The application tier needs to receive traffic from the web tier, which would be forwarded by the ALB after the initial HTTPS request from the user. Explanation: Option A is necessary because the web tier is the interface that users interact with, and it must be accessible via HTTPS from the ALB. This is a standard practice for web applications to ensure secure communication. Option C is essential for security, as it restricts access to the database tier, which is a common target for attacks. Only allowing the application tier

to communicate with the database tier helps to minimize the attack surface and follows the principle of least privilege. Option E is important because the application tier, which contains the business logic, needs to receive traffic from the web tier. This traffic would typically be forwarded by the ALB after the initial request from the user. The other options are not recommended for the following reasons: Option B is too permissive, as it allows the web tier to send outbound HTTPS traffic to any IP address, which is unnecessary and could pose a security risk. Option D is incorrect because the database tier should not need to send traffic to the web tier. The database should only receive connections, typically from the application tier. Option F is incorrect because the application tier should not need to send Microsoft SQL Server traffic to the web tier. The application tier communicates with the database tier, not the other way around. By choosing options A, C, and E, the solutions architect ensures that each tier can only receive and send the necessary traffic, maintaining a secure and efficient architecture.

解析: Correct Answer Combination and Explanation: A. Configure the security group for the web tier to allow inbound HTTPS traffic from the security group for the ALB. – Correct. The web tier needs to receive incoming HTTPS traffic from the ALB, which is the entry point for users over the internet. C. Configure the security group for the database tier to allow inbound Microsoft SQL Server traffic from the security group for the application tier. – Correct. The database tier should only accept traffic from the application tier, which contains the business logic that requires access to the database. E. Configure the security group for the application tier to allow inbound HTTPS traffic from the security group for the web tier. – Correct. The application tier needs to receive traffic from the web tier, which would be forwarded by the ALB after the initial HTTPS request from the user. Explanation: Option A is necessary because the web tier is the interface that users interact with, and it must be accessible via HTTPS from the ALB. This is a standard practice for web applications to ensure secure communication. Option C is essential for security, as it restricts access to the database tier, which is a common target for attacks. Only allowing the application tier

to communicate with the database tier helps to minimize the attack surface and follows the principle of least privilege. Option E is important because the application tier, which contains the business logic, needs to receive traffic from the web tier. This traffic would typically be forwarded by the ALB after the initial request from the user. The other options are not recommended for the following reasons: Option B is too permissive, as it allows the web tier to send outbound HTTPS traffic to any IP address, which is unnecessary and could pose a security risk. Option D is incorrect because the database tier should not need to send traffic to the web tier. The database should only receive connections, typically from the application tier. Option F is incorrect because the application tier should not need to send Microsoft SQL Server traffic to the web tier. The application tier communicates with the database tier, not the other way around. By choosing options A, C, and E, the solutions architect ensures that each tier can only receive and send the necessary traffic, maintaining a secure and efficient architecture.

108. Question #8851. 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.)
- 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.

答案：CD

解析：The correct combination is CD. The Compute Savings Plan (D) covers all three compute services used by the company: EC2, Lambda, and Fargate, which makes it the most efficient choice for covering multiple services. Additionally, purchasing a SageMaker Savings Plan (C) ensures coverage for the SageMaker service. Option A is less efficient as it only covers EC2 and SageMaker, leaving Lambda uncovered. Option B incorrectly

suggests the existence of a Compute Savings Plan that includes all three services, which is not the case.

解析: The correct combination is CD. The Compute Savings Plan (D) covers all three compute services used by the company: EC2, Lambda, and Fargate, which makes it the most efficient choice for covering multiple services. Additionally, purchasing a SageMaker Savings Plan (C) ensures coverage for the SageMaker service. Option A is less efficient as it only covers EC2 and SageMaker, leaving Lambda uncovered. Option B incorrectly suggests the existence of a Compute Savings Plan that includes all three services, which is not the case.

109. Question #886A 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.)

- 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.

答案: BC

解析: The correct combination is BC. Enabling Babelfish on Aurora PostgreSQL (B) allows the database to understand commands from applications written for Microsoft SQL Server, which minimizes the need for changes in the application code. Using the AWS Schema Conversion Tool (AWS SCT) (A) and AWS Database Migration Service (AWS DMS) (C) together provides a comprehensive solution for migrating the database schema and data with minimal changes to the application code. Option A alone would not be sufficient for data migration, and option D is not required as it

is used for read/write splitting and not for migration purposes.

解析: The correct combination is BC. Enabling Babelfish on Aurora PostgreSQL (B) allows the database to understand commands from applications written for Microsoft SQL Server, which minimizes the need for changes in the application code. Using the AWS Schema Conversion Tool (AWS SCT) (A) and AWS Database Migration Service (AWS DMS) (C) together provides a comprehensive solution for migrating the database schema and data with minimal changes to the application code. Option A alone would not be sufficient for data migration, and option D is not required as it is used for read/write splitting and not for migration purposes.

110. Question #900A 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.)

- 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.

答案: AB

解析: The correct combination is AB. Using an Application Load Balancer (B) is necessary for managing HTTP traffic to the ECS services. Setting up an ECS cluster with AWS Fargate (A) allows for running application

containers in the cloud without managing the underlying servers. Option A also includes using Amazon ECS Anywhere for on-premises containers, which is suitable for a hybrid environment. Option C's Network Load Balancer is not specified for HTTP traffic. Option D is less efficient because it suggests using Fargate for both cloud and on-premises, which is not necessary. Option E is incorrect because it mixes EC2 and Fargate launch types, which is not required.

解析: The correct combination is AB. Using an Application Load Balancer (B) is necessary for managing HTTP traffic to the ECS services. Setting up an ECS cluster with AWS Fargate (A) allows for running application containers in the cloud without managing the underlying servers. Option A also includes using Amazon ECS Anywhere for on-premises containers, which is suitable for a hybrid environment. Option C's Network Load Balancer is not specified for HTTP traffic. Option D is less efficient because it suggests using Fargate for both cloud and on-premises, which is not necessary. Option E is incorrect because it mixes EC2 and Fargate launch types, which is not required.

111. Question #905A 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.)

- 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.

答案：AD

解析：AD – TCP uses NLB for non-http use and an accelerator. This combination helps in improving the availability and performance of the hybrid application by efficiently handling the stateful TCP-based workload and the stateless UDP-based workload. (B) is not the best choice as CloudFront is more suitable for content delivery and may not be the optimal solution for this specific hybrid application. (C) and (E) using two load balancers may add complexity and is not necessary in this case. (D) is also a valid option, but AD is a more suitable combination for the given requirements.

解析：AD – TCP uses NLB for non-http use and an accelerator. This combination helps in improving the availability and performance of the hybrid application by efficiently handling the stateful TCP-based workload and the stateless UDP-based workload. (B) is not the best choice as CloudFront is more suitable for content delivery and may not be the optimal solution for this specific hybrid application. (C) and (E) using two load balancers may add complexity and is not necessary in this case. (D) is also a valid option, but AD is a more suitable combination for the given requirements.

112. Question #923A 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.)

- 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.

答案：BE

解析：To resolve the performance issue and improve application availability most cost-effectively, I recommend the following combination of steps:

- 1. Create an Amazon Machine Image (AMI) from the web server. Reference the AMI in a new launch template.
- 2. Create an Auto Scaling group and an Application Load Balancer to scale horizontally.

Here's why these steps are recommended:

- 1. Creating an AMI:
 - This captures the current state of your web server, including the application and its configurations.
 - The AMI can be used to launch multiple identical instances, which is crucial for horizontal scaling.
- 2. Horizontal scaling with Auto Scaling group and Application Load Balancer:
 - Horizontal scaling allows you to distribute the load across multiple instances, addressing the CPU utilization issue.
 - An Auto Scaling group automatically adjusts the number of instances based on demand, ensuring optimal performance during peak times and cost-efficiency during low-demand periods.
 - The Application Load Balancer distributes incoming traffic across multiple instances, improving availability and fault tolerance.

Benefits of this approach:

- Cost-effective: You only pay for the resources you need, as the Auto Scaling group can scale in during low-demand periods.
- Improved performance: Multiple instances can handle more requests, resolving the CPU utilization issue.
- Enhanced availability: If one instance fails, others can continue serving requests, improving overall application availability.

Best practices to consider:

- 1. Configure appropriate scaling policies based on CPU utilization or other relevant metrics.
- 2. Implement health checks to ensure the load balancer only routes traffic to healthy instances.
- 3. Use

AWS CloudWatch to monitor the performance of your scaled application and fine-tune your Auto Scaling policies as needed. 4. Consider implementing caching mechanisms or optimizing your application code to further improve performance. Sources [1] [Get instance type recommendations with AWS Compute Optimizer – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-getting-recommendations.html>) [3] [Get EC2 instance recommendations from Compute Optimizer – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recommendations.html>) [6] [Choose your scaling method – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling-overview.html>)

解析: To resolve the performance issue and improve application availability most cost-effectively, I recommend the following combination of steps:

1. Create an Amazon Machine Image (AMI) from the web server. Reference the AMI in a new launch template.
2. Create an Auto Scaling group and an Application Load Balancer to scale horizontally. Here's why these steps are recommended:
 - 1. Creating an AMI:
 - This captures the current state of your web server, including the application and its configurations.
 - The AMI can be used to launch multiple identical instances, which is crucial for horizontal scaling.
 - 2. Horizontal scaling with Auto Scaling group and Application Load Balancer:
 - Horizontal scaling allows you to distribute the load across multiple instances, addressing the CPU utilization issue.
 - An Auto Scaling group automatically adjusts the number of instances based on demand, ensuring optimal performance during peak times and cost-efficiency during low-demand periods.
 - The Application Load Balancer distributes incoming traffic across multiple instances, improving availability and fault tolerance.
- Benefits of this approach:
 - Cost-effective: You only pay for the resources you need, as the Auto Scaling group can scale in during low-demand periods.
 - Improved performance: Multiple instances can handle more requests, resolving the CPU utilization issue.
 - Enhanced availability: If one instance fails, others can continue serving requests, improving overall application availability.

Best practices to consider:

1. Configure appropriate scaling policies based on CPU

utilization or other relevant metrics. 2. Implement health checks to ensure the load balancer only routes traffic to healthy instances. 3. Use AWS CloudWatch to monitor the performance of your scaled application and fine-tune your Auto Scaling policies as needed. 4. Consider implementing caching mechanisms or optimizing your application code to further improve performance. Sources [1] [Get instance type recommendations with AWS Compute Optimizer – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-getting-recommendations.html>) [3] [Get EC2 instance recommendations from Compute Optimizer – Amazon Elastic Compute Cloud] (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recommendations.html>) [6] [Choose your scaling method – Amazon EC2 Auto Scaling] (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling-overview.html>)

113. Question #929A 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.)

- 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.

答案：ADF

解析：ADF – Creating a resource policy for the SNS topic that allows the Lambda function to publish messages to the topic (A) ensures that the Lambda function has the necessary permissions to interact with the SNS topic. Specifying the Lambda function's Amazon Resource Name (ARN) in the SNS topic's resource policy (D) further enhances the access control.

Configuring a Lambda execution role that has the necessary IAM permissions to use a customer managed key in AWS KMS (F) ensures that the Lambda function can securely access the encryption key for publishing messages to the encrypted SNS topic. (B) using server-side encryption with AWS KMS keys (SSE-KMS) instead of customer managed keys is not in line with the requirement of using customer managed keys for encryption. (C) creating a resource policy for the encryption key is not directly related to granting the Lambda function the necessary permissions to publish messages to the SNS topic. (E) associating an Amazon API Gateway HTTP API with the SNS topic is not necessary for this specific requirement.

解析：ADF – Creating a resource policy for the SNS topic that allows the Lambda function to publish messages to the topic (A) ensures that the Lambda function has the necessary permissions to interact with the SNS topic. Specifying the Lambda function's Amazon Resource Name (ARN) in the SNS topic's resource policy (D) further enhances the access control.

Configuring a Lambda execution role that has the necessary IAM permissions to use a customer managed key in AWS KMS (F) ensures that the Lambda function can securely access the encryption key for publishing messages to the encrypted SNS topic. (B) using server-side encryption with AWS KMS keys (SSE-KMS) instead of customer managed keys is not in line with the requirement of using customer managed keys for encryption. (C) creating a resource policy for the encryption key is not directly related to granting the Lambda function the necessary permissions to publish messages to the SNS topic. (E) associating an Amazon API Gateway HTTP API with the SNS topic is not necessary for this specific requirement.

114. Question #931A 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.)

- 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.

答案：AC

解析：AC – Creating an IAM resource policy for the Lambda function that allows Amazon SNS to invoke the function (A) ensures that the Lambda function can be triggered by messages from the SNS topic. Creating an IAM policy for the SNS topic that allows the Lambda function to subscribe to the topic (C) enables the necessary communication between the SNS topic and the Lambda function. (B) using an SQS queue to buffer messages and invoke the Lambda function adds unnecessary complexity. (D) using Amazon EventBridge rule to capture SNS topic notifications and forward them to the Lambda function is not the most direct way to achieve the

requirement. (E) storing performance metrics in an S3 bucket and using Amazon Athena to analyze them is not relevant to invoking the Lambda function based on SNS topic notifications.

解析：AC – Creating an IAM resource policy for the Lambda function that allows Amazon SNS to invoke the function (A) ensures that the Lambda function can be triggered by messages from the SNS topic. Creating an IAM policy for the SNS topic that allows the Lambda function to subscribe to the topic (C) enables the necessary communication between the SNS topic and the Lambda function. (B) using an SQS queue to buffer messages and invoke the Lambda function adds unnecessary complexity. (D) using Amazon EventBridge rule to capture SNS topic notifications and forward them to the Lambda function is not the most direct way to achieve the requirement. (E) storing performance metrics in an S3 bucket and using Amazon Athena to analyze them is not relevant to invoking the Lambda function based on SNS topic notifications.

115. Question #935A 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.)

- 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.

答案：BC

解析：To make the critical web application scalable, highly available, and reduce MySQL read latency, I recommend the following combination of solutions:

- 1. Implement Amazon Aurora MySQL-Compatible Edition:
 - Migrate the existing MySQL database to Amazon Aurora MySQL-Compatible Edition.
 - Aurora provides better scalability and performance compared to traditional MySQL.
 - It offers built-in read scaling capabilities, which can significantly reduce read latency.
 - Aurora's Multi-AZ deployment ensures high availability and automatic failover.
- 2. Use Auto Scaling with Application Load Balancer:
 - Move the application from a single EC2 instance to an Auto Scaling group.
 - Configure the Auto Scaling group to span multiple Availability Zones for high availability.
 - Set up an Application Load Balancer (ALB) to distribute traffic across the EC2 instances.
 - This configuration allows the application to scale horizontally based on demand. Additional best practices to consider:
 - Place the EC2 instances in private subnets for enhanced security, and use a NAT Gateway for outbound internet access if required.
 - Utilize Amazon Aurora Read Replicas to further distribute read traffic and improve performance.
 - Implement a caching layer using Amazon ElastiCache to reduce database load for frequently accessed data.
 - Use AWS Secrets Manager to securely manage database credentials and other sensitive information.
 - Regularly backup your Aurora database using automated snapshots.
 - Monitor your application and database performance using Amazon CloudWatch and set up appropriate alarms.

By implementing these solutions, you'll create a scalable, highly available architecture that can handle increased load and provide improved read performance for your critical web application.

ref: [1] [Scaling reads for your MySQL database with Amazon Aurora – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.ReadScaling.htm>)

1) [3] [Best practices for Aurora MySQL performance and scaling – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.BestPractices.Performance.html>) [6] [Managing performance and scaling for Amazon Aurora MySQL – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Performance.html>)

解析: To make the critical web application scalable, highly available, and reduce MySQL read latency, I recommend the following combination of solutions:

- 1. Implement Amazon Aurora MySQL-Compatible Edition:
 - Migrate the existing MySQL database to Amazon Aurora MySQL-Compatible Edition.
 - Aurora provides better scalability and performance compared to traditional MySQL.
 - It offers built-in read scaling capabilities, which can significantly reduce read latency.
 - Aurora's Multi-AZ deployment ensures high availability and automatic failover.
- 2. Use Auto Scaling with Application Load Balancer:
 - Move the application from a single EC2 instance to an Auto Scaling group.
 - Configure the Auto Scaling group to span multiple Availability Zones for high availability.
 - Set up an Application Load Balancer (ALB) to distribute traffic across the EC2 instances.
 - This configuration allows the application to scale horizontally based on demand. Additional best practices to consider:
 - Place the EC2 instances in private subnets for enhanced security, and use a NAT Gateway for outbound internet access if required.
 - Utilize Amazon Aurora Read Replicas to further distribute read traffic and improve performance.
 - Implement a caching layer using Amazon ElastiCache to reduce database load for frequently accessed data.
 - Use AWS Secrets Manager to securely manage database credentials and other sensitive information.
 - Regularly backup your Aurora database using automated snapshots.
 - Monitor your application and database performance using Amazon CloudWatch and set up appropriate alarms. By implementing these solutions, you'll create a scalable, highly available architecture that can handle increased load and provide improved read performance for your critical web application.

ref: [1] [Scaling reads for your MySQL database with Amazon Aurora – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.ReadScaling.html>)

1) [3] [Best practices for Aurora MySQL performance and scaling – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.BestPractices.Performance.html>) [6] [Managing performance and scaling for Amazon Aurora MySQL – Amazon Aurora] (<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Performance.html>)

116. Question #936 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.)

- 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

答案：CD

解析：CD – Storing sensitive information in AWS Secrets Manager (C) provides a secure and centralized way to store the information. AWS Secrets Manager also manages the automatic rotation of the sensitive information, reducing the operational overhead. Storing sensitive information in AWS Systems Manager Parameter Store (D) is another option, but it may not have the same level of built-in support for automatic rotation as AWS Secrets Manager. (A) Creating HTTP security headers by using Lambda@Edge to retrieve and create sensitive information may not be the most efficient or secure way to store and manage sensitive information for thousands of Lambda functions. (B) Creating a Lambda layer that retrieves sensitive information adds complexity and may not be the best approach for managing the automatic rotation of the information. (E) Creating a Lambda consumer with dedicated throughput to retrieve

sensitive information and create environmental variables is not a common or recommended approach for storing and managing sensitive information.

解析: CD – Storing sensitive information in AWS Secrets Manager (C) provides a secure and centralized way to store the information. AWS Secrets Manager also manages the automatic rotation of the sensitive information, reducing the operational overhead. Storing sensitive information in AWS Systems Manager Parameter Store (D) is another option, but it may not have the same level of built – in support for automatic rotation as AWS Secrets Manager. (A) Creating HTTP security headers by using Lambda@Edge to retrieve and create sensitive information may not be the most efficient or secure way to store and manage sensitive information for thousands of Lambda functions. (B) Creating a Lambda layer that retrieves sensitive information adds complexity and may not be the best approach for managing the automatic rotation of the information. (E) Creating a Lambda consumer with dedicated throughput to retrieve sensitive information and create environmental variables is not a common or recommended approach for storing and managing sensitive information.

117. Question #941A 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.)

- 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 ResourceName (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.

答案：DE

解析：DE – Defining an IAM role that includes the necessary permissions and annotating the Kubernetes service accounts with the Amazon ResourceName (ARN) of the IAM role (D) allows for granular access control of specific AWS resources for the Kubernetes service accounts. Setting up a trust relationship between the IAM roles for the service accounts and an OpenID Connect (OIDC) identity provider (E) ensures the security and authentication of the service accounts. (A) Attaching the IAM policy directly to the IAM role of the EKS nodes does not provide the granular access control required for the Kubernetes service accounts. (B) Implementing network policies within the EKS cluster to prevent access to specific AWS services is not the most effective way to manage access using IRSA. (C) Modifying the EKS cluster's IAM role to include permissions for each Kubernetes service account may not be the best practice as it can lead to complex and difficult – to – manage permissions.

解析：DE – Defining an IAM role that includes the necessary permissions and annotating the Kubernetes service accounts with the Amazon ResourceName (ARN) of the IAM role (D) allows for granular access control of specific AWS resources for the Kubernetes service accounts. Setting up a trust relationship between the IAM roles for the service accounts and an OpenID Connect (OIDC) identity provider (E) ensures the security and authentication of the service accounts. (A) Attaching the IAM policy directly to the IAM role of the EKS nodes does not provide the granular access control required for the Kubernetes service accounts. (B) Implementing network policies within the EKS cluster to prevent access to specific AWS services is not the most effective way to manage access using IRSA. (C) Modifying the EKS cluster's IAM role to include permissions for each Kubernetes service account may not be the best practice as it can lead to complex and difficult – to – manage permissions.

118. Question #957A 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 transit gateway to connect multiple VPCs. Which combination of steps will meet these requirements MOST cost - effectively? (Choose two.)

- 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.

答案：BD

解析：BD – Associating an AWS Direct Connect gateway with the transit gateway that is attached to the VPCs (B) provides a low - latency connection between the on - premises data centers and the AWS Cloud. Establishing an AWS Direct Connect connection and creating a transit virtual interface (VIF) to a Direct Connect gateway (D) further enhances the connectivity and ensures single - digit latencies for the workloads. This combination is the most cost - effective solution for meeting the requirements. (A) Establishing an AWS Site - to - Site VPN connection to each VPC may introduce higher latency and may not be suitable for workloads requiring single - digit latencies. (C) Establishing an AWS Site - to - Site VPN connection to an AWS Direct Connect gateway is not a common or recommended approach. (E) Associating AWS Site - to - Site VPN connections with the transit gateway may not provide the low - latency connectivity required for the workloads.

解析：BD – Associating an AWS Direct Connect gateway with the transit gateway that is attached to the VPCs (B) provides a low - latency connection between the on - premises data centers and the AWS Cloud. Establishing an AWS Direct Connect connection and creating a transit

virtual interface (VIF) to a Direct Connect gateway (D) further enhances the connectivity and ensures single - digit latencies for the workloads. This combination is the most cost - effective solution for meeting the requirements. (A) Establishing an AWS Site - to - Site VPN connection to each VPC may introduce higher latency and may not be suitable for workloads requiring single - digit latencies. (C) Establishing an AWS Site - to - Site VPN connection to an AWS Direct Connect gateway is not a common or recommended approach. (E) Associating AWS Site - to - Site VPN connections with the transit gateway may not provide the low - latency connectivity required for the workloads.

119. Question #973A 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.)

- 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.

答案: ACE

解析: Based on the requirements for the company's web application with an internet-facing Application Load Balancer (ALB), the correct combination of security group configurations for the ALB are: 1. A. Allow HTTPS inbound traffic from 0.0.0.0/0 for port 443. This allows the ALB to

receive HTTPS traffic from the public internet on the standard HTTPS port.

2. C. Allow HTTPS outbound traffic to the web application instances for port 443. This enables the ALB to forward HTTPS traffic to the web application servers on EC2 instances using port 443.

3. E. Allow HTTPS outbound traffic to the web application instances for the health check on port 8443. This allows the ALB to perform health checks on the web application servers using HTTPS on port 8443. These configurations ensure that:

- The ALB can receive incoming HTTPS traffic from the internet.
- The ALB can send HTTPS traffic to the web application servers on port 443.
- The ALB can perform health checks on the web application servers using HTTPS on port 8443.

It's important to note that these security group rules follow the principle of least privilege by allowing only the necessary inbound and outbound traffic for the ALB to function as required.

Best practices for implementing this configuration:

1. Use separate security groups for the ALB and the EC2 instances running the web application.
2. Configure the EC2 instances' security group to allow inbound HTTPS traffic only from the ALB's security group on ports 443 and 8443.
3. Regularly review and audit security group rules to ensure they remain aligned with the application's needs and security best practices.
4. Consider implementing AWS Web Application Firewall (WAF) with the ALB for additional layer of security against common web exploits.
5. Enable access logs for the ALB to monitor traffic patterns and detect potential security issues.

Remember to test these configurations in a non-production environment before implementing them in your production setup. Always refer to the latest AWS documentation for the most up-to-date information on security best practices and ALB configurations.

Sources

- [1] [Application Load Balancers – Elastic Load Balancing] (<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancers.html>)
- [3] [Security groups for the instances for your Classic Load Balancer – Elastic Load Balancing] (<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-instances-security-groups.html>)
- [6] [Security groups for your Application Load Balancer – Elastic Load Balancing] (<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html>)

解析: Based on the requirements for the company's web application with an internet-facing Application Load Balancer (ALB), the correct combination of security group configurations for the ALB are:

1. A. Allow HTTPS inbound traffic from 0.0.0.0/0 for port 443. This allows the ALB to receive HTTPS traffic from the public internet on the standard HTTPS port.
2. C. Allow HTTPS outbound traffic to the web application instances for port 443. This enables the ALB to forward HTTPS traffic to the web application servers on EC2 instances using port 443.
3. E. Allow HTTPS outbound traffic to the web application instances for the health check on port 8443. This allows the ALB to perform health checks on the web application servers using HTTPS on port 8443.

These configurations ensure that:

- The ALB can receive incoming HTTPS traffic from the internet.
- The ALB can send HTTPS traffic to the web application servers on port 443.
- The ALB can perform health checks on the web application servers using HTTPS on port 8443.

It's important to note that these security group rules follow the principle of least privilege by allowing only the necessary inbound and outbound traffic for the ALB to function as required.

Best practices for implementing this configuration:

1. Use separate security groups for the ALB and the EC2 instances running the web application.
2. Configure the EC2 instances' security group to allow inbound HTTPS traffic only from the ALB's security group on ports 443 and 8443.
3. Regularly review and audit security group rules to ensure they remain aligned with the application's needs and security best practices.
4. Consider implementing AWS Web Application Firewall (WAF) with the ALB for additional layer of security against common web exploits.
5. Enable access logs for the ALB to monitor traffic patterns and detect potential security issues.

Remember to test these configurations in a non-production environment before implementing them in your production setup. Always refer to the latest AWS documentation for the most up-to-date information on security best practices and ALB configurations.

Sources [1] [Application Load Balancers – Elastic Load Balancing] (<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancers.html>) [3] [Security groups for the instances for your Classic Load Balancer – Elastic Load Balancing] (<https://docs.aws.amazon.com>).

[com/elasticloadbalancing/latest/classic/elb-instances-security-groups.htm](https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-instances-security-groups.html)
l) [6] [Security groups for your Application Load Balancer – Elastic Load Balancing] (<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html>)

120. Question #974A 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.)

- 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.

答案：AD

解析：Based on the requirements, here are the two solutions that will meet the company's needs: 1. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront. 2. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC). Explanation: 1. For using a custom domain name with CloudFront, you need to use an SSL/TLS certificate. AWS Certificate Manager (ACM) is the recommended service for this purpose. However, when using ACM certificates with CloudFront, the certificate must be requested in the us-east-1 (N. Virginia) region, regardless of where your S3 bucket is located. This is because CloudFront is a global service and requires certificates to be in the us-east-1 region. 2. To allow secure uploads from CloudFront to your S3 bucket, you should use CloudFront origin access control (OAC). OAC is the recommended method for

restricting access to your S3 bucket so that it's only accessible through CloudFront. This provides an additional layer of security and ensures that users can only upload files through your CloudFront distribution. Best practices and additional considerations:

- When implementing OAC, make sure to update your S3 bucket policy to only allow access from your specific CloudFront distribution. This follows the principle of least privilege.
- Ensure that your S3 bucket has the "Block all public access" setting enabled to prevent direct access to the bucket.
- Consider enabling CloudFront field-level encryption for sensitive data if needed.
- Remember to configure CORS (Cross-Origin Resource Sharing) on your S3 bucket if your application requires it.
- Regularly review and rotate your ACM certificates to maintain security.
- Monitor your CloudFront and S3 access logs to detect any unusual activity. Always test your configuration in a non-production environment before implementing it in production.

For the most up-to-date information on CloudFront and S3 integration, please refer to the official AWS documentation. Sources

- [1] [Access control in Amazon S3 – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-management.html>) [3]
- [2] [Require HTTPS for communication between CloudFront and your Amazon S3 origin – Amazon CloudFront] (<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html>) [6]
- [3] [Ways to use CloudFront – Amazon CloudFront] (<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/IntroductionUseCases.html>)

解析: Based on the requirements, here are the two solutions that will meet the company's needs:

1. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront.
2. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC).

Explanation:

1. For using a custom domain name with CloudFront, you need to use an SSL/TLS certificate. AWS Certificate Manager (ACM) is the recommended service for this purpose. However, when using ACM certificates with CloudFront, the certificate must be requested in the us-east-1 (N. Virginia) region, regardless of where your S3 bucket is located. This is because CloudFront is a global service and requires certificates to be in the us-east-1 region.
2. To

allow secure uploads from CloudFront to your S3 bucket, you should use CloudFront origin access control (OAC). OAC is the recommended method for restricting access to your S3 bucket so that it's only accessible through CloudFront. This provides an additional layer of security and ensures that users can only upload files through your CloudFront distribution.

Best practices and additional considerations:

- When implementing OAC, make sure to update your S3 bucket policy to only allow access from your specific CloudFront distribution. This follows the principle of least privilege.
- Ensure that your S3 bucket has the "Block all public access" setting enabled to prevent direct access to the bucket.
- Consider enabling CloudFront field-level encryption for sensitive data if needed.
- Remember to configure CORS (Cross-Origin Resource Sharing) on your S3 bucket if your application requires it.
- Regularly review and rotate your ACM certificates to maintain security.
- Monitor your CloudFront and S3 access logs to detect any unusual activity. Always test your configuration in a non-production environment before implementing it in production.

For the most up-to-date information on CloudFront and S3 integration, please refer to the official AWS documentation. Sources

- [1] [Access control in Amazon S3 – Amazon Simple Storage Service] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-management.html>)
- [3] [Require HTTPS for communication between CloudFront and your Amazon S3 origin – Amazon CloudFront] (<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html>)
- [6] [Ways to use CloudFront – Amazon CloudFront] (<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/IntroductionUseCases.html>)

121. Question #987 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.)

- 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.

答案：AB

解析：Options A and B are the correct combination for achieving high availability and cost-effective scaling. Adding a Network Load Balancer (Option A) ensures that traffic is distributed across healthy EC2 instances, while configuring an Auto Scaling group (Option B) allows the application to automatically scale based on demand.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options A and B are the correct combination for achieving high availability and cost-effective scaling. Adding a Network Load Balancer (Option A) ensures that traffic is distributed across healthy EC2 instances, while configuring an Auto Scaling group (Option B) allows the application to automatically scale based on demand.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

122. Question #988 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.)

- 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.

答案：AD

解析：Options A and D are the correct combination for enforcing tagging requirements and preventing unauthorized actions. Creating a tag policy (Option A) ensures that all EC2 instances are tagged with the required data sensitivity values, and creating a service control policy (Option D) prevents the creation of untagged instances and the deletion of tags.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options A and D are the correct combination for enforcing tagging requirements and preventing unauthorized actions. Creating a tag policy (Option A) ensures that all EC2 instances are tagged with the required data sensitivity values, and creating a service control policy (Option D) prevents the creation of untagged instances and the deletion of tags.

答案供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

123. Question #1006A company uses AWS Systems Manager for routine management and patching of Amazon EC2 instances. The EC2 instances are in an IP address type target group behind an Application Load Balancer (ALB). New security protocols require the company to remove EC2 instances from service during a patch. When the company attempts to follow the security protocol during the next patch, the company receives errors during the patching window. Which combination of solutions will resolve the errors? (Choose two.)

- A. Change the target type of the target group from IP address type to instance type.
- B. Continue to use the existing Systems Manager document without changes because it is already optimized to handle instances that are in an IP address type target group behind an ALB.

- C. Implement the AWSEC2-PatchLoadBalancerInstance Systems Manager Automation document to manage the patching process.
- D. Use Systems Manager Maintenance Windows to automatically remove the instances from service to patch the instances.
- E. Configure Systems Manager State Manager to remove the instances from service and manage the patching schedule. Use ALB health checks to re-route traffic.

答案：CD

解析：Options C and D are the correct combination of solutions to resolve the errors encountered during the patching window. Implementing the AWSEC2-PatchLoadBalancerInstance Systems Manager Automation document (Option C) streamlines the patching process, and using Systems Manager Maintenance Windows (Option D) to automatically remove instances from service for patching, along with ALB health checks to re-route traffic, ensures compliance with security protocols.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options C and D are the correct combination of solutions to resolve the errors encountered during the patching window. Implementing the AWSEC2-PatchLoadBalancerInstance Systems Manager Automation document (Option C) streamlines the patching process, and using Systems Manager Maintenance Windows (Option D) to automatically remove instances from service for patching, along with ALB health checks to re-route traffic, ensures compliance with security protocols.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

124. Question #1010 A company runs multiple workloads on virtual machines (VMs) in an on-premises data center. The company is expanding rapidly. The on-premises data center is not able to scale fast enough to meet business needs. The company wants to migrate the workloads to AWS. The migration is time sensitive. The company wants to use a lift-and-shift strategy for non-critical workloads. Which combination of steps will meet these requirements? (Choose three.)

- A. Use the AWS Schema Conversion Tool (AWS SCT) to collect data about the VMs.

- B. Use AWS Application Migration Service. Install the AWS Replication Agent on the VMs.
- C. Complete the initial replication of the VMs. Launch test instances to perform acceptance tests on the VMs.
- D. Stop all operations on the VMs. Launch a cutover instance.
- E. Use AWS App2Container (A2C) to collect data about the VMs.
- F. Use AWS Database Migration Service (AWS DMS) to migrate the VMs.

答案：BCD

解析：Options B, C, and D are the correct combination of steps for a time-sensitive migration using a lift-and-shift strategy. Using AWS Application Migration Service and the AWS Replication Agent (Option B), completing initial replication and performing acceptance tests (Option C), and launching a cutover instance after stopping operations on the VMs (Option D) ensure a smooth migration process.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options B, C, and D are the correct combination of steps for a time-sensitive migration using a lift-and-shift strategy. Using AWS Application Migration Service and the AWS Replication Agent (Option B), completing initial replication and performing acceptance tests (Option C), and launching a cutover instance after stopping operations on the VMs (Option D) ensure a smooth migration process.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

125. Question #1011 A company hosts an application in a private subnet. The company has already integrated the application with Amazon Cognito. The company uses an Amazon Cognito user pool to authenticate users. The company needs to modify the application so the application can securely store user documents in an Amazon S3 bucket. Which combination of steps will securely integrate Amazon S3 with the application? (Choose two.)

- A. Create an Amazon Cognito identity pool to generate secure Amazon S3 access tokens for users when they successfully log in.
- B. Use the existing Amazon Cognito user pool to generate Amazon S3 access tokens for users when they successfully log in.

- C. Create an Amazon S3 VPC endpoint in the same VPC where the company hosts the application.
- D. Create a NAT gateway in the VPC where the company hosts the application. Assign a policy to the S3 bucket to deny any request that is not initiated from Amazon Cognito.
- E. Attach a policy to the S3 bucket that allows access only from the users' IP addresses.

答案：AC

解析：Options A and C are the correct combination of steps to securely integrate Amazon S3 with the application. Creating an Amazon Cognito identity pool to generate secure Amazon S3 access tokens (Option A) and creating an Amazon S3 VPC endpoint in the same VPC where the application is hosted (Option C) ensure secure access to S3 resources without exposing them to the public internet.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、

解析：Options A and C are the correct combination of steps to securely integrate Amazon S3 with the application. Creating an Amazon Cognito identity pool to generate secure Amazon S3 access tokens (Option A) and creating an Amazon S3 VPC endpoint in the same VPC where the application is hosted (Option C) ensure secure access to S3 resources without exposing them to the public internet.

答案与解析供参考，目前还在修正中，如有不同意见，请不吝指正，谢谢、