

Q1. An organization is currently hosting a large amount of frequently accessed data consisting of key-value pairs and semi-structured documents in their data center. They are planning to move this data to AWS. Which of one of the following services MOST effectively meets their needs?

- A. Amazon Redshift
- B. Amazon RDS
- C. Amazon DynamoDB
- D. Amazon Aurora

Q2 A Lambda function must execute a query against an Amazon RDS database in a private subnet.

Which steps are required to allow the Lambda function to access the Amazon RDS database? (Select two.)

- A. Create a VPC Endpoint for Amazon RDS.
- B. Create the Lambda function within the Amazon RDS VPC.
- C. Change the ingress rules of Lambda security group, allowing the Amazon RDS security group.
- D. Change the ingress rules of the Amazon RDS security group, allowing the Lambda security group.
- E. Add an Internet Gateway (IGW) to the VPC, route the private subnet to the IGW.

Q3. A Solutions Architect needs to build a resilient data warehouse using Amazon Redshift. The Architect needs to rebuild the Redshift cluster in another region.

Which approach can the Architect take to address this requirement?

- A. Modify the Redshift cluster and configure cross-region snapshots to the other region.
- B. Modify the Redshift cluster to take snapshots of the Amazon EBS volumes each day, sharing those snapshots with the other region.
- C. Modify the Redshift cluster and configure the backup and specify the Amazon S3 bucket in the other region.
- D. Modify the Redshift cluster to use AWS Snowball in export mode with data delivered to the other region.

Q4. A popular e-commerce application runs on AWS. The application encounters performance issues. The database is unable to handle the amount of queries and load during peak times. The database is running on the RDS Aurora engine on the largest instance size available.

What should an administrator do to improve performance?

- A. Convert the database to Amazon Redshift.
- B. Create a CloudFront distribution.
- C. Convert the database to use EBS Provisioned IOPS.
- D. Create one or more read replicas.

Q5. A Solutions Architect is designing the architecture for a new three-tier web-based e-commerce site that must be available 24/7. Requests are expected to range from 100 to 10,000 each minute. Usage can vary depending on time of day, holidays, and promotions. The design should be able to handle these volumes, with the ability to handle higher volumes if necessary.

How should the Architect design the architecture to ensure the web tier is cost-optimized and can handle the expected traffic? (Select two.)

- A. Launch Amazon EC2 instances in an Auto Scaling group behind an ELB.
- B. Store all static files in a multi-AZ Amazon Aurora database.
- C. Create an CloudFront distribution pointing to static content in Amazon S3.
- D. Use Amazon Route 53 to route traffic to the correct region.
- E. Use Amazon S3 multi-part uploads to improve upload times.

Q6. A Solution Architect is designing a three-tier web application. The Architect wants to restrict access to the database tier to accept traffic from the application servers only. However, these application servers are in an Auto Scaling group and may vary in quantity.

How should the Architect configure the database servers to meet the requirements?

- A. Configure the database security group to allow database traffic from the application server IP addresses.

B. Configure the database security group to allow database traffic from the application server security group.

C. Configure the database subnet network ACL to deny all inbound non-database traffic from the application-tier subnet.

D. Configure the database subnet network ACL to allow inbound database traffic from the application-tier subnet.

Q7 A Solutions Architect is designing a solution for a media company that will stream large amounts of data from an Amazon EC2 instance. The data streams are typically large and sequential, and must be able to support up to 500 MB/s. Which storage type will meet the performance requirements of this application?

- A. EBS Provisioned IOPS SSD
- B. EBS General Purpose SSD
- C. EBS Cold HDD
- D. EBS Throughput Optimized HDD

Q8. A legacy application running in premises requires a Solutions Architect to be able to open a firewall to allow access to several Amazon S3 buckets. The Architect has a VPN connection to AWS in place.

How should the Architect meet this requirement?

- A. Create an IAM role that allows access from the corporate network to Amazon S3.

- B. Configure a proxy on Amazon EC2 and use an Amazon S3 VPC endpoint.
- C. Use Amazon API Gateway to do IP whitelisting.
- D. Configure IP whitelisting on the customer's gateway.

Q9. A Solutions Architect is designing a database solution that must support a high rate of random disk reads and writes. It must provide consistent performance, and requires long-term persistence.

Which storage solution BEST meets these requirements?

- A. An Amazon EBS Provisioned IOPS volume
- B. An Amazon EBS General Purpose volume
- C. An Amazon EBS Magnetic volume
- D. An Amazon EC2 Instance Store

Q10. A Solutions Architect is designing solution with AWS Lambda where different environments require different database passwords.

What should the Architect do to accomplish this in a secure and scalable way?

- A. Create a Lambda function for each individual environment.
- B. Use Amazon DynamoDB to store environmental variables.
- C. Use encrypted AWS Lambda environmental variables.
- D. Implement a dedicated Lambda function for distributing variables.

Answer C

Analyze:

A Solutions Architect is designing a highly-available website that is served by multiple web servers hosted outside of AWS. If an instance becomes unresponsive, the Architect needs to remove it from the rotation. What is the MOST efficient way to fulfill this requirement?

- A. Use Amazon CloudWatch to monitor utilization.
- B. Use Amazon API Gateway to monitor availability.
- C. Use an Amazon Elastic Load Balancer.
- D. Use Amazon Route 53 health checks.

Q11 A company hosts a popular web application. The web application connects to a database running in a private VPC subnet. The web servers must be accessible only to customers on an SSL connection. The RDS MySQL database server must be accessible only from the web servers.

How should the Architect design a solution to meet the requirements without impacting running applications?

- A. Create a network ACL on the web server's subnet, and allow HTTPS inbound and MySQL outbound.

Place both database and web servers on the same subnet.

- B. Open an HTTPS port on the security group for web servers and set the source to 0.0.0.0/0. Open the MySQL port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group.

C. Create a network ACL on the web server's subnet, and allow HTTPS inbound, and specify the source as 0.0.0.0/0. Create a network ACL on a database subnet, allow MySQL port inbound for web servers, and deny all outbound traffic.

D. Open the MySQL port on the security group for web servers and set the source to 0.0.0.0/0. Open the HTTPS port on the database security group and attach it to the MySQL instance. Set the source to Web Server Security Group.

Q12. Which service should an organization use if it requires an easily managed and scalable platform to host its web application running on Nginx?

- A. AWS Lambda
- B. Auto Scaling
- C. AWS Elastic Beanstalk
- D. Elastic Load Balancing

Q13. Developers are creating a new online transaction processing (OLTP) application for a small database that is very read-write intensive. A single table in the database is updated continuously throughout the day, and the developers want to ensure that the database performance is consistent. Which Amazon EBS storage option will achieve the MOST consistent performance to help maintain application performance?

- A. Provisioned IOPS SSD

- B. General Purpose SSD
- C. Cold HDD
- D. Throughput Optimized HDD

Q14. A Solutions Architect is designing a log-processing solution that requires storage that supports up to 500 MB/s throughput. The data is sequentially accessed by an Amazon EC2 instance.

Which Amazon storage type satisfies these requirements?

- A. EBS Provisioned IOPS SSD (io1)
- B. EBS General Purpose SSD (gp2)
- C. EBS Throughput Optimized HDD (st1)
- D. EBS Cold HDD (sc1)

Q15. A company's development team plans to create an Amazon S3 bucket that contains millions of images. The team wants to maximize the read performance of Amazon S3.

Which naming scheme should the company use?

- A. Add a date as the prefix.
- B. Add a sequential id as the suffix.
- C. Add a hexadecimal hash as the suffix.
- D. Add a hexadecimal hash as the prefix.



Q16. A Solutions Architect needs to design a solution that will enable a security team to detect, review, and perform root cause analysis of security incidents that occur in a cloud environment. The Architect must provide a centralized view of all API events for current and future AWS regions.

How should the Architect accomplish this task?

- A. Enable AWS CloudTrail logging in each individual region. Repeat this for all future regions.
- B. Enable Amazon CloudWatch logs for all AWS services across all regions and aggregate them in a single Amazon S3 bucket.
- C. Enable AWS Trusted Advisor security checks and report all security incidents for all regions.
- D. Enable AWS CloudTrail by creating a new trail and apply the trail to all regions.

Q17. A company has a legacy application using a proprietary file system and plans to migrate the application to AWS.

Which storage service should the company use?

- A. Amazon DynamoDB
- B. Amazon S3
- C. Amazon EBS
- D. Amazon EFS

Q18. A company plans to use AWS for all new batch processing workloads.

The company's developers use Docker containers for the new batch processing. The system design must accommodate critical and non-critical batch processing workloads 24/7.

How should a Solutions Architect design this architecture in a cost-efficient manner?

- A. Purchase Reserved Instances to run all containers. Use Auto Scaling groups to schedule jobs.
- B. Host a container management service on Spot Instances. Use Reserved Instances to run Docker containers.
- C. Use Amazon ECS orchestration and Auto Scaling groups: one with Reserve Instances, one with Spot Instances.
- D. Use Amazon ECS to manage container orchestration. Purchase Reserved Instances to run all batch workloads at the same time.

Q19. A company is evaluating Amazon S3 as a data storage solution for their daily analyst reports. The company has implemented stringent requirements concerning the security of the data at rest. Specifically, the CISO asked for the use of envelope encryption with separate permissions for the use of an envelope key, automated rotation of the encryption keys, and visibility into when an encryption key was used and by whom.

Which steps should a Solutions Architect take to satisfy the security requirements requested by the CISO?

- A. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with Customer- Provided Keys (SSE-C).
- B. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with Amazon S3- Managed Keys (SSE-S3).
- C. Create an Amazon S3 bucket to store the reports and use Server-Side Encryption with AWS KMS- Managed Keys (SSE-KMS).
- D. Create an Amazon S3 bucket to store the reports and use Amazon s3 versioning with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).

A customer has a production application that frequently overwrites and deletes data, the application requires the most up-to-date version of the data every time it is requested. Which storage should a Solutions Architect recommend to bet accommodate this use case?

- A. Amazon S3
- B. Amazon RDS
- C. Amazon RedShift
- D. AWS Storage Gateway

Q20. A Solutions Architect has five web servers serving requests for a domain.Which of the following Amazon Route 53 routing policies can distribute traffic randomly among all healthy web servers?

- A. Simple

- B. Failover
- C. Weighted
- D. Multivalue

Q21.An online events registration system is hosted in AWS and uses ECS to host its front-end tier and an RDS configured with Multi-AZ for its database tier. What are the events that will make Amazon RDS automatically perform a failover to the standby replica? (Select TWO.)

- A. In the event of Read Replica failure
- B. Compute unit failure on secondary DB instance
- C. Loss of availability in primary Availability Zone
- D. Storage failure on primary
- E. Storage failure on secondary DB instance

Q22.A financial company wants to store their data in Amazon S3 but at the same time, they want to store their frequently accessed data locally on their on-premises server. This is due to the fact that they do not have the option to extend their on-premises storage, which is why they are looking for adurable and scalable storage service to use in AWS.

- A. Use Amazon Glacier
- B. Use both Elasticache and S3 for frequently accessed data
- C. Use a fleet of EC2 instance with EBS volumes to store the commonly used

data

#### D. Use the Amazon Storage Gateway - Cached Volumes

Q23. A multinational manufacturing company has multiple accounts in AWS to separate their various departments such as finance, human resources, engineering and many others. There is a requirement to ensure that certain access to services and actions are properly controlled to comply with the security policy of the company. As the Solutions Architect, which is the most suitable way to set up the multi-account AWS environment of the company?

A. Provide access to externally authenticated users via Identity Federation. Set up an IAM role to specify permissions for users from each department whose identity is federated from your organization or a third-party identity provider.

B. Connect all departments by setting up a cross-account access to each of the AWS accounts of the company. Create and attach IAM policies to your resources based on their respective departments to control access.

C. Set up a common IAM policy that can be applied across all AWS accounts.

D. Use AWS Organizations and Service Control Policies to control services on each account.

Q24 A company launched a global news website that is deployed to AWS and is using MySQL RDS. The website has millions of viewers from all over the world which means that the website has read-heavy database workloads. All

database transactions must be ACID compliant to ensure data integrity. In this scenario, which of the following is the best option to use to increase the read throughput on the MySQL database?

- A. Enable Amazon RDS Standby Replicas
- B. Enable Amazon RDS Read Replicas
- C. Use SQS to queue up the requests
- D. Enable Multi-AZ deployments

Q25.A startup plans to develop a multiplayer game that uses UDP as the protocol for communication between clients and game servers. The data of the users will be stored in a key-value store. As the Solutions Architect, you need to implement a solution that will distribute the traffic across a number of servers.

- A. Distribute the traffic using Network Load Balancer and store the data in Amazon Aurora.
- B. Distribute the traffic using Application Load Balancer and store the data in Amazon DynamoDB.
- C. Distribute the traffic using Network Load Balancer and store the data in Amazon DynamoDB.
- D. Distribute the traffic using Application Load Balancer and store the data in Amazon RDS.

Q26. A tech company currently has an on-premises infrastructure. They are currently running low on storage and want to have the ability to extend their storage using the AWS cloud.Which AWS service can help them achieve this requirement?

- A. Amazon Elastic Block Storage
- B. Amazon Storage Gateway
- C. Amazon EC2
- D. Amazon SQS

Q27.A large multinational investment bank has a web application that requires a minimum of 4 EC2 instances to run to ensure that it can cater to its users across the globe. You are instructed to ensure fault tolerance of this system.Which of the following is the best option?

- A. Deploy an Auto Scaling group with 4 instances in one Availability Zone behind an Application Load Balancer.
- B. Deploy an Auto Scaling group with 1 instance in each of 4 Availability Zones behind an Application Load Balancer.
- C. Deploy an Auto Scaling group with 2 instances in each of 3 Availability Zones behind an Application Load Balancer.
- D. Deploy an Auto Scaling group with 2 instances in each of 2 Availability Zones behind an Application Load Balancer.

Q28 A company wishes to query data that resides in multiple AWS accounts from a central data lake. Each account has its own Amazon S3 bucket that stores data unique to its business function. Users from different accounts must be granted access to the data lake based on their roles. Which solution will minimize overhead and costs while meeting the required access patterns?

- A. Use AWS Central Tower to centrally manage each account's S3 buckets.
- B. Create a scheduled Lambda function for transferring data from multiple accounts to the S3 buckets of a central account
- C. Use AWS Kinesis Firehose to consolidate data from multiple accounts into a single account.
- D. Use AWS Lake Formation to consolidate data from multiple accounts into a single account.

Q29 A media company needs to configure an Amazon S3 bucket to serve static assets for the public-facing web application. Which methods ensure that all of the objects uploaded to the S3 bucket can be read publicly all over the Internet?

(Select TWO.)

- A. Create an IAM role to set the objects inside the S3 bucket to public read.
- B. Configure the cross-origin resource sharing (CORS) of the S3 bucket to allow objects to be publicly accessible from all domains.
- C. Do nothing. Amazon S3 objects are already public by default.
- D. Configure the S3 bucket policy to set all objects to public read.



E. Grant public read access to the object when uploading it using the S3 Console.

Q30. Both historical records and frequently accessed data are stored on an on-premises storage system. The amount of current data is growing at an exponential rate. As the storage's capacity is nearing its limit, the company's Solutions Architect has decided to move the historical records to AWS to free up space for the active data. Which of the following architectures deliver the best solution in terms of cost and operational management?

A. Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.

B. Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier Deep Archive to be the destination for the data.

C. Use AWS DataSync to move the historical records from on-premises to AWS. Choose Amazon S3 Standard to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon S3 Glacier Deep Archive after 30 days.

D. Use AWS Storage Gateway to move the historical records from on-premises to AWS. Choose Amazon S3 Glacier to be the destination for the data. Modify the S3 lifecycle configuration to move the data from the Standard tier to Amazon

S3 Glacier Deep Archive after 30 days.

Q31.A multinational company has been building its new data analytics platform with high-performance computing workloads (HPC) which requires a scalable, POSIX-compliant storage service.The data need to be stored redundantly across multiple AZs and allows concurrent connections from thousands of EC2 instances hosted on multiple Availability Zones.Which of the following AWS storage service is the most suitable one to use in this scenario?

- A. Amazon ElastiCache
- B. Amazon Elastic File System
- C. Amazon EBS Volumes
- D. Amazon S3

Q32.A company needs to implement a solution that will process real-time streaming data of its users across the globe. This will enable them to track and analyze globally-distributed user activity on their website and mobile applications, including clickstream analysis. The solution should process the data in close geographical proximity to their users and respond to user requests at low latencies.Which of the following is the most suitable solution for this scenario?

- A. Integrate CloudFront with Lambda@Edge in order to process the data in

close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Amazon Athena and durably store the results to an Amazon S3 bucket.

B. Use a CloudFront web distribution and Route 53 with a Geoproximity routing policy in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

C. Integrate CloudFront with Lambda@Edge in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

D. Use a CloudFront web distribution and Route 53 with a latency-based routing policy, in order to process the data in close geographical proximity to users and respond to user requests at low latencies. Process real-time streaming data using Kinesis and durably store the results to an Amazon S3 bucket.

Q33.A company hosted a web application on a Linux Amazon EC2 instance in the public subnet that uses a default network ACL. The instance uses a default security group and has an attached Elastic IP address. The network ACL has been configured to block all traffic to the instance. The Solutions Architect must allow incoming traffic on port 443 to access the application from any source. Which combination of steps will accomplish this requirement? (Select

TWO.)

A. In the Security Group, add a new rule to allow TCP connection on port 443 from source 0.0.0.0/0

B. In the Security Group, create a new rule to allow TCP connection on port 443 to destination 0.0.0.0/0

C. In the Network ACL, update the rule to allow outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0

D. In the Network ACL, update the rule to allow both inbound and outbound TCP connection on port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0

E. In the Network ACL, update the rule to allow inbound TCP connection on port 443 from source 0.0.0.0/0 and outbound TCP connection on port 32768 - 65535 to destination 0.0.0.0/0

Q34. A company developed a web application and deployed it on a fleet of EC2 instances that uses Amazon SQS. The requests are saved as messages in the SQS queue, which is configured with the maximum message retention period. However, after thirteen days of operation, the web application suddenly crashed and there are 10,000 unprocessed messages that are still waiting in the queue. Since they developed the application, they can easily resolve the issue but they need to send a communication to the users on the issue. What information should they provide and what will happen to the unprocessed messages?

A. Tell the users that unfortunately, they have to resubmit all of the requests

since the queue would not be able to process the 10,000 messages together.

B. Tell the users that the application will be operational shortly however, requests sent over three days ago will need to be resubmitted.

C. Tell the users that unfortunately, they have to resubmit all the requests again.

D. Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted.

Q35. A company has an On-Demand EC2 instance with an attached EBS volume. There is a scheduled job that creates a snapshot of this EBS volume every midnight at 12 AM when the instance is not used. One night, there has been a production incident where you need to perform a change on both the instance and on the EBS volume at the same time when the snapshot is currently taking place. Which of the following scenario is true when it comes to the usage of an EBS volume while the snapshot is in progress?

A. The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes

B. The EBS volume can be used in read-only mode while the snapshot is in progress.

C. The EBS volume cannot be used until the snapshot completes.

D. The EBS volume can be used while the snapshot is in progress.

Q36. There is a new compliance rule in your company that audits every

Windows and Linux EC2 instances each month to view any performance issues. They have more than a hundred EC2 instances running in production, and each must have a logging function that collects various system details regarding that instance. The SysOps team will periodically review these logs and analyze their contents using AWS Analytics tools, and the result will need to be retained in an S3 bucket. In this scenario, what is the most efficient way to collect and analyze logs from the instances with minimal effort?

A. Install AWS Inspector Agent in each instance which will collect and push data to CloudWatch Logs periodically. Set up a CloudWatch dashboard to properly analyze the log data of all instances.

B. Install AWS SDK in each instance and create a custom daemon script that would collect and push data to CloudWatch Logs periodically. Enable CloudWatch detailed monitoring and use CloudWatch Logs Insights to analyze the log data of all instances.

C. Install the AWS Systems Manager Agent (SSM Agent) in each instance which will automatically collect and push data to CloudWatch Logs. Analyze the log data with CloudWatch Logs Insights.

D. Install the unified CloudWatch Logs agent in each instance which will automatically collect and push data to CloudWatch Logs. Analyze the log data with CloudWatch Logs Insights.

Q37.An online cryptocurrency exchange platform is hosted in AWS which uses

ECS Cluster and RDS in MultiAZ Deployments configuration. The application is heavily using the RDS instance to process complex read and write database operations. To maintain the reliability, availability, and performance of your systems, you have to closely monitor how the different processes or threads on a DB instance use the CPU, including the percentage of the CPU bandwidth and total memory consumed by each process. Which of the following is the most suitable solution to properly monitor your database?

- A. Create a script that collects and publishes custom metrics to CloudWatch, which tracks the real-time CPU Utilization of the RDS instance, and then set up a custom CloudWatch dashboard to view the metrics.
- B. Check the CPU% and MEM% metrics which are readily available in the Amazon RDS console that shows the percentage of the CPU bandwidth and total memory consumed by each database process of your RDS instance.
- C. Enable Enhanced Monitoring in RDS.
- D. Use Amazon CloudWatch to monitor the CPU Utilization of your database.

Q38. A company is hosting an application on EC2 instances that regularly pushes and fetches data in Amazon S3. Due to a change in compliance, the instances need to be moved on a private subnet. Along with this change, the company wants to lower the data transfer costs by configuring its AWS resources. How can this be accomplished in the MOST cost-efficient manner?

- A. Create an Amazon S3 gateway endpoint to enable a connection between

the instances and Amazon S3.

B. Set up an AWS Transit Gateway to access Amazon S3.

C. Set up a NAT Gateway in the public subnet to connect to Amazon S3.

D. Create an Amazon S3 interface endpoint to enable a connection between the instances and Amazon S3.

Q39.A company is using AWS IAM to manage access to AWS services. The

Solutions Architect of the company created the following IAM policy for AWS

Lambda: { "Version": "2012-10-17", "Statement": [{"Effect": "Allow", "Action": ["lambda:CreateFunction", "lambda:DeleteFunction"], "Resource": "\*"}, {"Effect": "Deny", "Action":

["lambda:CreateFunction", "lambda:DeleteFunction", "lambda:InvokeFunction", "lambda:TagResource"], "Resource": "\*", "Condition": {"IpAddress": {"aws:SourceIp": "187.5.104.11/32"}}}]}

Which of the following options are allowed by this policy?

A. Create an AWS Lambda function using the 187.5.104.11/32 address.

B. Create an AWS Lambda function using the 100.220.0.11/32 address.

C. Delete an AWS Lambda function using the 187.5.104.11/32 address.

D. Delete an AWS Lambda function from any network address.

Q40. A tech company has a CRM application hosted on an Auto Scaling group

of On-Demand EC2 instances. The application is extensively used during office



hours from 9 in the morning till 5 in the afternoon. Their users are complaining that the performance of the application is slow during the start of the day but then works normally after a couple of hours. Which of the following can be done to ensure that the application works properly at the beginning of the day?

- A. Configure a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day.
- B. Set up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances.
- C. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization.
- D. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization.

Q41. A company decided to change its third-party data analytics tool to a cheaper solution. They sent a full data export on a CSV file which contains all of their analytics information. You then save the CSV file to an S3 bucket for storage. Your manager asked you to do some validation on the provided data export. In this scenario, what is the most cost-effective and easiest way to analyze export data using standard SQL?

- A. Use mysqldump client utility to load the CSV export file from S3 to a MySQL RDS instance. Run some SQL queries once the data has been loaded to complete your validation.

B. To be able to run SQL queries, use AWS Athena to analyze the export data file in S3.

C. Create a migration tool to load the CSV export file from S3 to a DynamoDB instance. Once the data has been loaded, run queries using DynamoDB.

D. Use a migration tool to load the CSV export file from S3 to a database that is designed for online analytic processing (OLAP) such as AWS RedShift. Run some queries once the data has been loaded to complete your validation.

Q42.A company generates large financial datasets with millions of rows. The Solutions Architect needs to store all the data in a columnar fashion to reduce the number of disk I/O requests and reduce the amount of data needed to load from the disk. The bank has an existing third-party business intelligence application that will connect to the storage service and then generate daily and monthly financial reports for its clients around the globe. In this scenario, which is the best storage service to use to meet the requirement?

A. Amazon Aurora

B. Amazon RDS

C. Amazon DynamoDB

D. Amazon Redshift

Q43. A company is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are

connecting to the VPC over the Internet to manage the fleet of Amazon EC2 instances running in both the public and private subnets. The Solutions Architect has added a bastion host with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC. Which of the following bastion host deployment options will meet this requirement?

- A. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
- B. Deploy a Windows Bastion host on the corporate network that has RDP access to all EC2 instances in the VPC.
- C. Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow RDP access to bastion only from the corporate IP addresses.
- D. Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.

Q44. A company has a serverless application made up of AWS Amplify, Amazon API Gateway and a Lambda function. The application is connected to an Amazon RDS MySQL database instance inside a private subnet. A Lambda Function URL is also implemented as the dedicated HTTPS endpoint for the function, which has the following value: `https://12june1898pil1pinas.lambda-url.us-west-2.on.aws/` There are times during peak loads

when the database throws a "too many connections" error preventing the users from accessing the application. Which solution could the company take to resolve the issue?

- A. Increase the memory allocation of the Lambda function
- B. Provision an RDS Proxy between the Lambda function and RDS database instance
- C. Increase the rate limit of API Gateway
- D. Increase the concurrency limit of the Lambda function

Q45. A company is building an internal application that processes loans, accruals, and interest rates for their clients. They require a storage service that is able to handle future increases in storage capacity of up to 16 TB and can provide the lowest-latency access to their data. The web application will be hosted in a single m5ad.24xlarge Reserved EC2 instance that will process and store data to the storage service. Which of the following storage services would you recommend?

- A. EFS
- B. S3
- C. EBS
- D. Storage Gateway

Q46. A Solutions Architect is designing a highly available environment for an

application. She plans to host the application on EC2 instances within an Auto Scaling Group. One of the conditions requires data stored on root EBS volumes to be preserved if an instance terminates. What should be done to satisfy the requirement?

- A. Use AWS DataSync to replicate root volume data to Amazon S3.
- B. Configure ASG to suspend the health check process for each EC2 instance.
- C. Set the value of DeleteOnTermination attribute of the EBS volumes to False.
- D. Enable the Termination Protection option for all EC2 instances.

Q47 A company has a static corporate website hosted in a standard S3 bucket and a new web domain name that was registered using Route 53. You are instructed by your manager to integrate these two services in order to successfully launch their corporate website. What are the prerequisites when routing traffic using Amazon Route 53 to a website that is hosted in an Amazon S3 Bucket? (Select TWO.)

- A. The record set must be of type "MX"
- B. The S3 bucket name must be the same as the domain name
- C. The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket
- D. A registered domain name
- E. The S3 bucket must be in the same region as the hosted zone

Q48. A Solutions Architect is designing a monitoring application which generates audit logs of all operational activities of the company's cloud infrastructure. Their IT Security and Compliance team mandates that the application retain the logs for 5 years before the data can be deleted. How can the Architect meet the above requirement?

- A. Store the audit logs in a Glacier vault and use the Vault Lock feature.
- B. Store the audit logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the S3 bucket.
- C. Store the audit logs in an EBS volume and then take EBS snapshots every month.
- D. Store the audit logs in an EFS volume and use Network File System version 4 (NFSv4) file-locking mechanism.

Q49. A company conducted a surprise IT audit on all of the AWS resources being used in the production environment. During the audit activities, it was noted that you are using a combination of Standard and Convertible Reserved EC2 instances in your applications. Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances? (Select TWO.)

- A. Convertible Reserved Instances allow you to exchange for another convertible reserved instance of a different instance family.
- B. It runs in a VPC on hardware that's dedicated to a single customer.

C. Unused Standard Reserved Instances can later be sold at the Reserved Instance Marketplace.

D. It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration.

E. Unused Convertible Reserved Instances can later be sold at the Reserved Instance Marketplace.

Q50.A company has a web-based ticketing service that utilizes Amazon SQS and a fleet of EC2 instances. The EC2 instances that consume messages from the SQS queue are configured to poll the queue as often as possible to keep end-to-end throughput as high as possible. The Solutions Architect noticed that polling the queue in tight loops is using unnecessary CPU cycles, resulting in increased operational costs due to empty responses. In this scenario, what should the Solutions Architect do to make the system more cost-effective?

A. Configure Amazon SQS to use short polling by setting the `ReceiveMessageWaitTimeSeconds` to zero.

B. Configure Amazon SQS to use long polling by setting the `ReceiveMessageWaitTimeSeconds` to a number greater than zero.

C. Configure Amazon SQS to use long polling by setting the `ReceiveMessageWaitTimeSeconds` to zero.

D. Configure Amazon SQS to use short polling by setting the `ReceiveMessageWaitTimeSeconds` to a number greater than zero.

Q51. A customer is transitioning their ActiveMQ messaging broker service onto the AWS cloud in which they require an alternative asynchronous service that supports NMS and MQTT messaging protocol. The customer does not have the time and resources needed to recreate their messaging service in the cloud. The service has to be highly available and should require almost no management overhead. Which of the following is the most suitable service to use to meet the above requirement?

- A. AWS Step Functions
- B. Amazon MQ
- C. Amazon SNS
- D. Amazon SWF

Q52. A company has an e-commerce application that saves the transaction logs to an S3 bucket. You are instructed by the CTO to configure the application to keep the transaction logs for one month for troubleshooting purposes, and then afterward, purge the logs. What should you do to accomplish this requirement?

- A. Add a new bucket policy on the Amazon S3 bucket.
- B. Enable CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data
- C. Create a new IAM policy for the Amazon S3 bucket that automatically deletes



the logs after a month

D. Configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month

Q53. A company plans to reduce the amount of data that Amazon S3 transfers to the servers in order to lower the operating costs as well as lower the latency of retrieving the data. To accomplish this, you need to use simple structured query language (SQL) statements to filter the contents of Amazon S3 objects and retrieve just the subset of data that you need. Which of the following services will help you accomplish this requirement?

A. Redshift Spectrum

B. RDS

C. S3 Select

D. AWS Step Functions

Q54. For data privacy, a healthcare company has been asked to comply with the Health Insurance Portability and Accountability Act (HIPAA). The company stores all its backups on an Amazon S3 bucket. It is required

Amazon S3 Select works on objects stored in CSV, JSON, or Apache Parquet format. It also works with objects that are compressed with GZIP or BZIP2 (for CSV and JSON objects only), and server-side encrypted objects. You can specify the format of the results as either CSV or JSON, and you can determine

how the records in the result are delimited. RDS is incorrect. Although RDS is an SQL database where you can perform SQL operations, it is still not valid because you want to apply SQL transactions on S3 itself, and not on the database, which RDS cannot do. Redshift Spectrum is incorrect. Although Amazon Redshift Spectrum provides a similar in-query functionality like S3 Select, this service is more suitable for querying your data from the Redshift external tables hosted in S3. The Redshift queries are run on your cluster resources against local disk. Redshift Spectrum queries run using per-query scale-out resources against data in S3 which can entail additional costs compared with S3 Select. AWS Step Functions is incorrect because this only lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.

that data stored on the S3 bucket must be encrypted.What is the best option to do this? (Select TWO.)

- A. Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys.
- B. Store the data on EBS volumes with encryption enabled instead of using Amazon S3.
- C. Enable Server-Side Encryption on an S3 bucket to make use of AES-128 encryption.
- D. Store the data in encrypted EBS snapshots.
- E. Enable Server-Side Encryption on an S3 bucket to make use of AES-256

encryption.

Q55.A Solutions Architect is designing a setup for a database that will run on Amazon RDS for MySQL. He needs to ensure that the database can automatically failover to an RDS instance to continue operating in the event of failure. The architecture should also be as highly available as possible. Which among the following actions should the Solutions Architect do?

A. Create five read replicas across different availability zones. In the event of an Availability Zone outage, promote any replica to become the primary instance.

B. Create five cross-region read replicas in each region. In the event of an Availability Zone outage, promote any replica to become the primary instance.

C. Create a standby replica in another availability zone by enabling Multi-AZ deployment.

D. Create a read replica in the same region where the DB instance resides. In addition, create a read replica in a different region to survive a region's failure. In the event of an Availability Zone outage, promote any replica to become the primary instance.

Q56. A company plans to migrate its suite of containerized applications running on-premises to a container service in AWS. The solution must be cloud-agnostic and use an open-source platform that can automatically manage

containerized workloads and services. It should also use the same configuration and tools across various production environments. What should the Solution Architect do to properly migrate and satisfy the given requirement?

A. Migrate the application to Amazon Elastic Kubernetes Service with EKS worker nodes.

B. Migrate the application to Amazon Elastic Container Service with ECS tasks that use the AWS Fargate launch type.

C. Migrate the application to Amazon Elastic Container Service with ECS tasks that use the Amazon EC2 launch type.

D. Migrate the application to Amazon Container Registry (ECR) with Amazon EC2 instance worker nodes.

Q57.A company plans to host a movie streaming app in AWS. The chief information officer (CIO) wants to ensure that the application is highly available and scalable. The application is deployed to an Auto Scaling group of EC2 instances on multiple AZs. A load balancer must be configured to distribute incoming requests evenly to all EC2 instances across multiple Availability Zones.Which of the following features should the Solutions Architect use to satisfy these criteria?

A. Path-based Routing

B. Amazon VPC IP Address Manager (IPAM)

C. Cross-zone load balancing

## D. AWS Direct Connect SiteLink

Q58.A Solutions Architect needs to ensure that all of the AWS resources in Amazon VPC don't go beyond their respective service limits. The Architect should prepare a system that provides real-time guidance in provisioning resources that adheres to the AWS best practices.Which of the following is the MOST appropriate service to use to satisfy this task?

- A. AWS Cost Explorer
- B. Amazon Inspector
- C. AWS Budgets
- D. AWS Trusted Advisor

Q59.A global medical research company has a molecular imaging system that provides each client with frequently updated images of what is happening inside the human body at the molecular and cellular levels. The system is hosted in AWS and the images are hosted in an S3 bucket behind a CloudFront web distribution. When a fresh batch of images is uploaded to S3, it is required to keep the previous ones in order to prevent them from being overwritten.Which of the following is the most suitable solution to solve this issue?

- A. Invalidate the files in your CloudFront web distribution
- B. Add a separate cache behavior path for the content and configure a custom object caching with a Minimum TTL of 0

- C. Add Cache-Control no-cache, no-store, or private directives in the S3 bucket
- D. Use versioned objects

Q60. A Solutions Architect is working for a financial company. The manager wants to have the ability to automatically transfer obsolete data from their S3 bucket to a low-cost storage system in AWS. What is the best solution that the Architect can provide to them?

- A. Use CloudEndure Migration.
- B. Use an EC2 instance and a scheduled job to transfer the obsolete data from their S3 location to Amazon S3 Glacier.
- C. Use Lifecycle Policies in S3 to move obsolete data to Glacier.
- D. Use Amazon SQS.

Q61. A software development company is using serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. They have a Lambda function that connects to a MongoDB Atlas, which is a popular Database as a Service (DBaaS) platform and also uses a third party API to

fetch certain data for their application. One of the developers was instructed to create the environment variables for the MongoDB database hostname, username, and password as well as the API credentials that will be used by the Lambda function for DEV, SIT, UAT, and PROD environments. Considering

that the Lambda function is storing sensitive database and API credentials, how can this information be secured to prevent other developers in the team, or anyone, from seeing these credentials in plain text? Select the best option that provides maximum security.

- A. Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information.
- B. AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead.
- C. There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service.
- D. Create a new KMS key and use it to enable encryption helpers that leverage on AWS Key Management Service to store and encrypt the sensitive information.

Q62. A company hosted an e-commerce website on an Auto Scaling group of EC2 instances behind an Application Load Balancer. The Solutions Architect noticed that the website is receiving a large number of illegitimate external requests from multiple systems with IP addresses that constantly change. To resolve the performance issues, the Solutions Architect must implement a solution that would block the illegitimate requests with minimal impact on legitimate traffic.

Which of the following options fulfills this requirement?

- A. Create a regular rule in AWS WAF and associate the web ACL to an Application Load Balancer.
- B. Create a rate-based rule in AWS WAF and associate the web ACL to an Application Load Balancer.
- C. Create a custom rule in the security group of the Application Load Balancer to block the offending requests.
- D. Create a custom network ACL and associate it with the subnet of the Application Load Balancer to block the offending requests.

Q63. There was an incident in your production environment where the user data stored in the S3 bucket has been accidentally deleted by one of the Junior DevOps Engineers. The issue was escalated to your manager and after a few days, you were instructed to improve the security and protection of your AWS resources. What combination of the following options will protect the S3 objects in your bucket from both accidental deletion and overwriting? (Select TWO.)

- A. Enable Versioning
- B. Enable Amazon S3 Intelligent-Tiering
- C. Provide access to S3 data strictly through pre-signed URL only
- D. Enable Multi-Factor Authentication Delete
- E. Disallow S3 Delete using an IAM bucket policy



Q64. A telecommunications company is planning to give AWS Console access to developers. Company policy mandates the use of identity federation and role-based access control. Currently, the roles are already assigned using groups in the corporate Active Directory. In this scenario, what combination of the following services can provide developers access to the AWS console?

(Select TWO.)

- A. AWS Directory Service Simple AD
- B. IAM Roles
- C. IAM Groups
- D. AWS Directory Service AD Connector
- E. Lambda

Q65. An AI-powered Forex trading application consumes thousands of data sets to train its machine learning model. The application's workload requires a high-performance, parallel hot storage to process the training datasets concurrently. It also needs cost-effective cold storage to archive those datasets that yield low profit.

Which of the following Amazon storage services should the developer use?

- A. Use Amazon FSx For Windows File Server and Amazon S3 for hot and cold storage respectively.
- B. Use Amazon Elastic File System and Amazon S3 for hot and cold storage respectively.

C. Use Amazon FSx For Lustre and Amazon EBS Provisioned IOPS SSD (io1) volumes for hot and cold storage respectively.

D. Use Amazon FSx For Lustre and Amazon S3 for hot and cold storage respectively.

Q66. A newly hired Solutions Architect is assigned to manage a set of CloudFormation templates that are used in the company's cloud architecture in AWS. The Architect accessed the templates and tried to analyze the configured IAM policy for an S3 bucket.

What does the above IAM policy allow? (Choose three.)

```
{  
  "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",  
  "Action": ["s3:Get*", "s3:List*"],  
  "Resource": "*" }  
},  
{ "Effect": "Allow",  
  "Action": "s3:PutObject",  
  "Resource": "arn:aws:s3:::boracay/*" }  
]  
}
```

A. An IAM user with this IAM policy is allowed to read objects in the boracay S3 bucket but not allowed to list the objects in the bucket.

B. An IAM user with this IAM policy is allowed to change access rights for the boracay S3 bucket.

C. An IAM user with this IAM policy is allowed to write objects into the boracay S3 bucket.

D. An IAM user with this IAM policy is allowed to read objects from the boracay S3 bucket.

E. An IAM user with this IAM policy is allowed to read and delete objects from the boracay S3 bucket.

F. An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.

Q67. A retail website has intermittent, sporadic, and unpredictable transactional workloads throughout the day that are hard to predict. The website is currently hosted on-premises and is slated to be migrated to AWS. A new relational database is needed that autoscales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over. Which of the following option is the MOST cost-effective and suitable database setup in this scenario?

A. Launch a DynamoDB Global table with Auto Scaling enabled.

B. Launch an Amazon Aurora Serverless DB cluster then set the minimum and maximum capacity for the cluster.

C. Launch an Amazon Redshift data warehouse cluster with Concurrency Scaling.

D. Launch an Amazon Aurora Provisioned DB cluster with burstable performance DB instance class types.

Q68. A popular social media website uses a CloudFront web distribution to serve their static contents to their millions of users around the globe. They are receiving a number of complaints recently that their users take a lot of time to log into their website. There are also occasions when their users are getting HTTP 504 errors. You are instructed by your manager to significantly reduce the user's login time to further optimize the system. Which of the following options should you use together to set up a cost-effective solution that can improve your application's performance? (Select TWO.)

A. Customize the content that the CloudFront web distribution delivers to your users using Lambda@Edge, which allows your Lambda functions to execute the authentication process in AWS locations closer to the users.

B. Deploy your application to multiple AWS regions to accommodate your users around the world. Set up a Route 53 record with latency routing policy to route incoming traffic to the region that provides the best latency to the user.

C. Configure your origin to add a Cache-Control max-age directive to your objects, and specify the longest practical value for max-age to increase the cache hit ratio of your CloudFront distribution.

D. Set up an origin failover by creating an origin group with two origins. Specify one as the primary origin and the other as the second origin which CloudFront

automatically switches to when the primary origin returns specific HTTP status code failure responses.

E. Use multiple and geographically disperse VPCs to various AWS regions then create a transit VPC to connect all of your resources. In order to handle the requests faster, set up Lambda functions in each region using the AWS Serverless Application Model (SAM) service.

Q69. A popular mobile game uses CloudFront, Lambda, and DynamoDB for its backend services. The player data is persisted on a DynamoDB table and the static assets are distributed by CloudFront. However, there are a lot of complaints that saving and retrieving player information is taking a lot of time. To improve the game's performance, which AWS service can you use to reduce DynamoDB response times from milliseconds to microseconds?

- A. DynamoDB Auto Scaling
- B. Amazon ElastiCache
- C. AWS Device Farm
- D. Amazon DynamoDB Accelerator (DAX)

Q70. A popular social network is hosted in AWS and is using a DynamoDB table as its database. There is a requirement to implement a 'follow' feature where users can subscribe to certain updates made by a particular user and be notified via email. Which of the following is the most suitable solution that you

should implement to meet the requirement?

A. Using the Kinesis Client Library (KCL), write an application that leverages on DynamoDB Streams Kinesis Adapter that will fetch data from the DynamoDB Streams endpoint. When there are updates made by a particular user, notify the subscribers via email using SNS.

B. Enable DynamoDB Stream and create an AWS Lambda trigger, as well as the IAM role which contains all of the permissions that the Lambda function will need at runtime. The data from the stream record will be processed by the Lambda function which will then publish a message to SNS Topic that will notify the subscribers via email.

C. Set up a DAX cluster to access the source DynamoDB table. Create a new DynamoDB trigger and a Lambda function. For every update made in the user data, the trigger will send data to the Lambda function which will then notify the subscribers via email using SNS.

D. Create a Lambda function that uses DynamoDB Streams Kinesis Adapter which will fetch data from the DynamoDB Streams endpoint. Set up an SNS Topic that will notify the subscribers via email when there is an update made by a particular user.

Q71. A suite of web applications is hosted in an Auto Scaling group of EC2 instances across three Availability Zones and is configured with default settings.

There is an Application Load Balancer that forwards the request to the

respective target group on the URL path. The scale-in policy has been triggered due to the low number of incoming traffic to the application.

Which EC2 instance will be the first one to be terminated by your Auto Scaling group?

- A. The EC2 instance launched from the oldest launch configuration
- B. The instance will be randomly selected by the Auto Scaling group
- C. The EC2 instance which has the least number of user sessions
- D. The EC2 instance which has been running for the longest time

Q72. A financial application is composed of an Auto Scaling group of EC2 instances, an Application Load Balancer, and a MySQL RDS instance in a Multi-AZ Deployments configuration. To protect the confidential data of your customers, you have to ensure that your RDS database can only be accessed using the profile credentials specific to your EC2 instances via an authentication token. As the Solutions Architect of the company, which of the following should you do to meet the above requirement?

- A. Create an IAM Role and assign it to your EC2 instances which will grant exclusive access to your RDS instance.
- B. Enable the IAM DB Authentication.
- C. Configure SSL in your application to encrypt the database connection to RDS.
- D. Use a combination of IAM and STS to restrict access to your RDS instance

via a temporary token.

Q73 A pharmaceutical company has resources hosted on both their on-premises network and in AWS cloud. They want all of their Software Architects to access resources on both environments using their on-premises credentials, which is stored in Active Directory. In this scenario, which of the following can be used to fulfill this requirement?

- A. Set up SAML 2.0-Based Federation by using a Web Identity Federation.
- B. Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).
- C. Use Amazon VPC
- D. Use IAM users

Q74. A company has 3 DevOps engineers that are handling its software development and infrastructure management processes. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service.

What can the DevOps engineers do to prevent this from happening again?

- A. Set up a signed URL for all users.
- B. Use S3 Infrequently Accessed storage to store the data.
- C. Create an IAM bucket policy that disables delete operation.
- D. Enable S3 Versioning and Multi-Factor Authentication Delete on the



bucket.(Correct)

Q75. An application that records weather data every minute is deployed in a fleet of Spot EC2 instances and uses a MySQL RDS database instance. Currently, there is only one RDS instance running in one Availability Zone. You plan to improve the database to ensure high availability by synchronous data replication to another RDS instance.

Which of the following performs synchronous data replication in RDS?

- A. CloudFront running as a Multi-AZ deployment
- B. DynamoDB Read Replica
- C. RDS DB instance running as a Multi-AZ deployment
- D. RDS Read Replica

Q76. A Solutions Architect identified a series of DDoS attacks while monitoring the VPC. The Architect needs to fortify the current cloud infrastructure to protect the data of the clients. Which of the following is the most suitable solution to mitigate these kinds of attacks?

- A. Use AWS Shield Advanced to detect and mitigate DDoS attacks.
- B. A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC.
- C. Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic.

D. Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks, and other DDoS attacks.

Q77. A travel photo sharing website is using Amazon S3 to serve high-quality photos to visitors of your website. After a few days, you found out that there are other travel websites linking and using your photos. This resulted in financial losses for your business.

What is the MOST effective method to mitigate this issue?

- A. Use CloudFront distributions for your photos.
- B. Block the IP addresses of the offending websites using NACL.
- C. Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.
- D. Store and privately serve the high-quality photos on Amazon WorkDocs instead.

Q78. The company that you are working for has a highly available architecture consisting of an elastic load balancer and several EC2 instances configured with auto-scaling in three Availability Zones. You want to monitor your EC2 instances based on a particular metric, which is not readily available in CloudWatch. Which of the following is a custom metric in CloudWatch which you have to manually set up?

- A. Network packets out of an EC2 instance

- B. CPU Utilization of an EC2 instance
- C. Disk Reads activity of an EC2 instance
- D. Memory Utilization of an EC2 instance

Q79. A Solutions Architect needs to make sure that the On-Demand EC2 instance can only be accessed from this IP address (110.238.98.71) via an SSH connection. Which configuration below will satisfy this requirement?

- A. Security Group Inbound Rule: Protocol -- UDP, Port Range -22, Source238.98.71/32
- B. Security Group Inbound Rule: Protocol -- TCP. Port Range -22, Source238.98.71/0
- C. Security Group Inbound Rule: Protocol -- TCP. Port Range -22, Source238.98.71/32
- D. Security Group Inbound Rule: Protocol -- UDP, Port Range -22, Source238.98.71/0

Q80. A government entity is conducting a population and housing census in the city. Each household information uploaded on their online portal is stored in encrypted files in Amazon S3. The government assigned its Solutions Architect to set compliance policies that verify sensitive data in a manner that meets their compliance standards. They should also be alerted if there are compromised files detected containing personally identifiable information (PII), protected

health information (PHI) or intellectual properties (IP). Which of the following should the Architect implement to satisfy this requirement?

- A. Set up and configure Amazon Macie to monitor and detect usage patterns on their Amazon S3 data.
- B. Set up and configure Amazon Inspector to send out alert notifications whenever a security violation is detected on their Amazon S3 data.
- C. Set up and configure Amazon Rekognition to monitor and recognize patterns on their Amazon S3 data.
- D. Set up and configure Amazon GuardDuty to monitor malicious activity on their Amazon S3 data.

Q81. An IT consultant is working for a large financial company. The role of the consultant is to help the development team build a highly available web application using stateless web servers. In this scenario, which AWS services are suitable for storing session state data? (Select TWO.)

- A. RDS
- B. Redshift Spectrum
- C. DynamoDB
- D. Glacier
- E. ElastiCache

Q82. A company has a web application that uses Internet Information Services

(IIS) for Windows Server. A file share is used to store the application data on the network-attached storage of the company's on-premises data center. To achieve a highly available system, they plan to migrate the application and file share to AWS.

Which of the following can be used to fulfill this requirement?

- A. Migrate the existing file share configuration to AWS Storage Gateway.
- B. Migrate the existing file share configuration to Amazon FSx for Windows File Server.
- C. Migrate the existing file share configuration to Amazon EFS.
- D. Migrate the existing file share configuration to Amazon EBS.

Q83. A company plans to migrate its on-premises workload to AWS. The current architecture is composed of a Microsoft SharePoint server that uses a Windows shared file storage. The Solutions Architect needs to use a cloud storage solution that is highly available and can be integrated with Active Directory for access control and authentication.

Which of the following options can satisfy the given requirement?

- A. Create a Network File System (NFS) file share using AWS Storage Gateway.
- B. Create a file system using Amazon FSx for Windows File Server and join it to an Active Directory domain in AWS.
- C. Launch an Amazon EC2 Windows Server to mount a new S3 bucket as a file volume.

D. Create a file system using Amazon EFS and join it to an Active Directory domain.

Q84. A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The database credentials should be supplied using environment variables, to comply with strict security compliance. As the Solutions Architect, you have to ensure that the credentials are secure and that they cannot be viewed in plaintext on the cluster itself.

Which of the following is the most suitable solution in this scenario that you can implement with minimal effort?

A. In the ECS task definition file of the ECS Cluster, store the database credentials using Docker Secrets to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Secrets are encrypted during transit and at rest. A given secret is only accessible to those services which have been granted explicit access to it via IAM Role, and only while those service tasks are running.

B. Use the AWS Systems Manager Parameter Store to keep the database credentials and then encrypt them using AWS KMS. Create an IAM Role for your Amazon ECS task execution role (taskRoleArn) and reference it with your task definition, which allows access to both KMS and the Parameter Store.

Within your container definition, specify secrets with the name of the

C. environment variable to set in the container and the full ARN of the Systems

Manager Parameter Store parameter containing the sensitive data to present to the container.

D. C. Store the database credentials in the ECS task definition file of the ECS Cluster and encrypt it with KMS. Store the task definition JSON file in a private S3 bucket and ensure that HTTPS is enabled on the bucket to encrypt the data in-flight. Create an IAM role to the ECS task definition script that allows access to the specific S3 bucket and then pass the `--cli-input-json` parameter when calling the ECS `register-task-definition`. Reference the task definition JSON file in the S3 bucket which contains the database credentials.

E. D. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS KMS. Create a resource-based policy for your Amazon ECS task execution role (`taskRoleArn`) and reference it with your task definition which allows access to both KMS and AWS Secrets Manager.

Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of the Secrets Manager secret which contains the sensitive data, to present to the container.

Q85. A company needs to deploy at least 2 EC2 instances to support the normal workloads of its application and automatically scale up to 6 EC2 instances to handle the peak load. The architecture must be highly available and fault-tolerant as it is processing mission-critical workloads. As the Solutions Architect of the company, what should you do to meet the above requirement?

A. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Use 2 Availability Zone and deploy 1 instances for each AZ.

B. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 4. Deploy 2 instances in Availability Zone A and 2 instances in Availability Zone B

C. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 2 and the maximum capacity to 6. Deploy 4 instances in Availability Zone A .

D. Create an Auto Scaling group of EC2 instances and set the minimum capacity to 4 and the maximum capacity to 6. Deploy 2 instances in Availability Zone A and another 2 instances in Availability Zone B

Q86. A Docker application, which is running on an Amazon ECS cluster behind a load balancer, is heavily using DynamoDB. You are instructed to improve the database performance by distributing the workload evenly and using the provisioned throughput efficiently.

Which of the following would you consider to implement for your DynamoDB table?

A. Use partition keys with low-cardinality attributes, which have a few number of distinct values for each item.

B. Reduce the number of partition keys in the DynamoDB table.



C. Use partition keys with high-cardinality attributes, which have a large number of distinct values for each item.

D. Avoid using a composite primary key, which is composed of a partition key and a sort key.

Q87. An organization needs to provision a new Amazon EC2 instance with a persistent block storage volume to migrate data from its on-premises network to AWS. The required maximum performance for the storage volume is 64,000 IOPS.

In this scenario, which of the following can be used to fulfill this requirement?

A. Launch an Amazon EFS file system and mount it to a Nitro-based Amazon EC2 instance and set the performance mode to Max I/O.

B. Directly attach multiple Instance Store volumes in an EC2 instance to deliver maximum IOPS performance.

C. Launch a Nitro-based EC2 instance and attach a Provisioned IOPS SSD EBS volume (io1) with 64,000 IOPS.

D. Launch any type of Amazon EC2 instance and attach a Provisioned IOPS SSD EBS volume (io1) with 64,000 IOPS.

Q88. A Solutions Architect designed a serverless architecture that allows AWS Lambda to access an Amazon DynamoDB table named tutorialsdojo in the US East (N. Virginia) region. The IAM policy attached to a Lambda function allows

it to put and delete items in the table. The policy must be updated to only allow two operations in the tutorialsdojo table and prevent other DynamoDB tables from being modified. Which of the following IAM policies fulfill this requirement and follows the principle of granting the least privilege?

A.

```
{"Version": "2012-10-17"
```

```
  "Statement": [
```

```
    {
```

```
      "Sid": "TutorialsdojoTablePolicy1",
```

```
      "Effect": "Allow",
```

```
      "Action": [
```

```
        "dynamodb:PutItem",
```

```
        "dynamodb:DeleteItem"
```

```
      ]
```

```
      "Resource": "arn:aws:dynamodb:us-east-1:1286189812061898:tab1/tutorialsdojo"
```

```
    },
```

```
  ]
```

```
  {
```

```
    "Sid": "TutorialsdojoTablePolicy2",
```

```
    "Effect": "Allow",
```

```
    "Action": "dynamodb:*",
```

```
    "Resource": "arn:aws:dynamodb:us-east-1:1286189812061898:tab1/tutorialsdojo"
```

east-1:1206189812061898:tab1e/tutorialsdojo"

]]}

B.

{"Version":"2012-10-17",

"Statement":[

{"Sid": "TutorialsdojoTablePolicy",

"Effect": "Allow",

"Action": [

"dynamodb:PutItem",

"dynamodb :DeleteItem"

]

"Resource": "arn:aws:dynamodb:us

east-1:120618981206:tab1e/tutorialsdojo"]}]}

C.

"Version": "2012-10-17",

"Statement": [

{"sid": "TutorialsdojoTablePolicy",

"Effect": "Allow",

\*Action": [

"dynamodb:PutItem",

"dynamodb :DeleteItem"

]

"Resource": "arn:aws:dynamodb:us-east-1:120618981206:table/"

D.

Version": "2012-10-17.

"Statement": [

    "sid": "Tutorialsdoyotablepolicy1",

    "Effect": "Allow",

    "Action": [

        "adom(",

        "dynamodb:PutItem",

        "dynamodb:DeleteItem"

]

"Resource": "arn:aws:dynamodb:us-east-

1:1206189812861898:t1e/tutorialsdoyio"

}

"Sid": "TutorialsdoyotablePolicy2",

"Effect": "Deny",

"Action": "dynamodb:\*\*",

"Resource": "arn:aws:dynamodb:us-east-1:1206189812061898:table/\*\*"

Q89. A company requires all the data stored in the cloud to be encrypted at rest. To easily integrate this with other AWS services, they must have full

control over the encryption of the created keys and also the ability to immediately remove the key material from AWS KMS. The solution should also be able to audit the key usage independently of AWS CloudTrail.

Which of the following options will meet this requirement?

- A. Use AWS Key Management Service to create a CMK in a custom key store and store the non- extractable key material in Amazon S3.
- B. Use AWS Key Management Service to create AWS-owned CMKs and store the non-extractable key material in AWS CloudHSM.
- C. Use AWS Key Management Service to create AWS-managed CMKs and store the non-extractable key material in AWS CloudHSM.
- D. Use AWS Key Management Service to create a CMK in a custom key store and store the non- extractable key material in AWS CloudHSM.

Q90. An application hosted in EC2 consumes messages from an SQS queue and is integrated with SNS to send out an email to you once the process is complete. The Operations team received 5 orders but after a few hours, they saw 20 email notifications in their inbox.

Which of the following could be the possible culprit for this issue?

- A. The web application is not deleting the messages in the SQS queue after it has processed them.
- B. The web application is set for long polling so the messages are being sent twice.

C. The web application does not have permission to consume messages in the SQS queue.

D. The web application is set to short polling so some messages are not being picked up

Q91. A Solutions Architect needs to set up a relational database and come up with a disaster recovery plan to mitigate multi-region failure. The solution requires a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute.

Which of the following AWS services can fulfill this requirement?

A. AWS Global Accelerator

B. Amazon Aurora Global Database

C. Amazon RDS for PostgreSQL with cross-region read replicas

D. Amazon DynamoDB global tables

Q92. A Solutions Architect is hosting a website in an Amazon S3 bucket named tutorialsdojo. The users load the website using the following URL: <http://tutorialsdojo.s3-website-us-east-1.amazonaws.com> and there is a new requirement to add a JavaScript on the webpages in order to make authenticated HTTP GET requests against the same bucket by using the Amazon S3 API endpoint ([tutorialsdojo.s3.amazonaws.com](http://tutorialsdojo.s3.amazonaws.com)). Upon testing, you noticed that the web browser blocks JavaScript from allowing those requests.

Which of the following options is the MOST suitable solution that you should implement for this scenario?

- A. Enable Cross-Region Replication (CRR).
- B. Enable Cross-origin resource sharing (CORS) configuration in the bucket.
- C. Enable cross-account access.
- D. Enable Cross-Zone Load Balancing.

Q93. A multi-tiered application hosted in your on-premises data center is scheduled to be migrated to AWS. The application has a message broker service which uses industry standard messaging APIs and protocols that must be migrated as well, without rewriting the messaging code in your application. Which of the following is the most suitable service that you should use to move your messaging service to AWS?

- A. Amazon SNS
- B. Amazon MQ
- C. Amazon SWF
- D. Amazon SQS

Q94. A company hosts multiple applications in their VPC. While monitoring the system, they noticed that multiple port scans are coming in from a specific IP address block that is trying to connect to several AWS resources inside their VPC. The internal security team has requested that all offending IP addresses

be denied for the next 24 hours for security purposes.

Which of the following is the best method to quickly and temporarily deny access from the specified IP addresses?

- A. Configure the firewall in the operating system of the EC2 instances to deny access from the IP address block.
- B. Add a rule in the Security Group of the EC2 instances to deny access from the IP Address block.
- C. Modify the Network Access Control List associated with all public subnets in the VPC to deny access from the IP Address block.
- D. Create a policy in IAM to deny access from the IP Address block.

Q95. A Forex trading platform, which frequently processes and stores global financial data every minute, is hosted in your on-premises data center and uses an Oracle database. Due to a recent cooling problem in their data center, the company urgently needs to migrate their infrastructure to AWS to improve the performance of their applications. As the Solutions Architect, you are responsible in ensuring that the database is properly migrated and should remain available in case of database server failure in the future. Which of the following is the most suitable solution to meet the requirement?

- A. Create an Oracle database in RDS with Multi-AZ deployments.
- B. Launch an Oracle Real Application Clusters (RAC) in RDS.
- C. Launch an Oracle database instance in RDS with Recovery Manager



(RMAN) enabled.

D. Convert the database schema using the AWS Schema Conversion Tool and AWS Database Migration Service. Migrate the Oracle database to a non-cluster Amazon Aurora with a single instance.

Q96. An application is hosted in an AWS Fargate cluster that runs a batch job whenever an object is loaded on an Amazon S3 bucket. The minimum number of ECS Tasks is initially set to 1 to save on costs, and it will only increase the task count based on the new objects uploaded on the S3 bucket. Once processing is done, the bucket becomes empty and the ECS Task count should be back to 1. Which is the most suitable option to implement with the LEAST amount of effort?

A. Set up an alarm in CloudWatch to monitor CloudTrail since the S3 object-level operations are recorded on CloudTrail. Create two Lambda functions for increasing/decreasing the ECS task count. Set these as respective targets for the CloudWatch Alarm depending on the S3 event.

B. Set up a CloudWatch Event rule to detect S3 object PUT operations and set the target to a Lambda function that will run Amazon ECS API command to increase the number of tasks on ECS. Create another rule to detect S3 DELETE operations and run the Lambda function to reduce the number of ECS tasks.

C. Set up a CloudWatch Event rule to detect S3 object PUT operations and set

the target to the ECS cluster with the increased number of tasks. Create another rule to detect S3 DELETE operations and set the target to the ECS Cluster with 1 as the Task count.

D. Set up an alarm in CloudWatch to monitor CloudTrail since this S3 object-level operations are recorded on CloudTrail. Set two alarm actions to update ECS task count to scale-out/scale- in depending on the S3 event.

Q97. In a government agency that you are working for, you have been assigned to put confidential tax documents on AWS cloud. However, there is a concern from a security perspective on what can be put on AWS. What are the features in AWS that can ensure data security for your confidential documents? (Select TWO.)

- A. Public Data Set Volume Encryption
- B. S3 On-Premises Data Encryption
- C. S3 Server-Side Encryption
- D. EBS On-Premises Data Encryption
- E. S3 Client-Side Encryption

Q98. A car dealership website hosted in Amazon EC2 stores car listings in an Amazon Aurora database managed by Amazon RDS. Once a vehicle has been sold, its data must be removed from the current listings and forwarded to a distributed processing system.

Which of the following options can satisfy the given requirement?

- A. Create an RDS event subscription and send the notifications to AWS Lambda. Configure the Lambda function to fan out the event notifications to multiple Amazon SQS queues to update the processing system.
- B. Create an RDS event subscription and send the notifications to Amazon SNS. Configure the SNS topic to fan out the event notifications to multiple Amazon SQS queues. Process the data using Lambda functions.
- C. Create a native function or a stored procedure that invokes a Lambda function. Configure the Lambda function to send event notifications to an Amazon SQS queue for the processing system to consume.
- D. Create an RDS event subscription and send the notifications to Amazon SQS. Configure the SQS queues to fan out the event notifications to multiple Amazon SNS topics. Process the data using Lambda functions.

Q99. An organization needs a persistent block storage volume that will be used for mission-critical workloads. The backup data will be stored in an object storage service and after 30 days, the data will be stored in a data archiving storage service.

What should you do to meet the above requirement?

- A. Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to

Amazon S3 One Zone-IA.

B. Attach an EBS volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.

C. Attach an instance store volume in your EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 One Zone-IA.

D. Attach an instance store volume in your existing EC2 instance. Use Amazon S3 to store your backup data and configure a lifecycle policy to transition your objects to Amazon S3 Glacier.

Q100. A Solutions Architect is working for a company which has multiple VPCs in various AWS regions. The Architect is assigned to set up a logging system which will track all of the changes made to their AWS resources in all regions, including the configurations made in IAM, CloudFront, AWS WAF, and Route 53. In order to pass the compliance requirements, the solution must ensure the security, integrity, and durability of the log data. It should also provide an event history of all API calls made in AWS Management Console and AWS CLI.

Which of the following solutions is the best fit for this scenario?

A. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--include-global-service-events` parameters then encrypt log files using KMS encryption.

Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

B. Set up a new CloudWatch trail in a new S3 bucket using the CloudTrail console and also pass the `--is-multi-region-trail` parameter then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

C. Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--include-global-service-events` parameters then encrypt log files using KMS encryption.

Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

D. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and also pass both the `--is-multi-region-trail` and `--no-include-global-service-events` parameters then encrypt log files using KMS encryption. Apply Multi Factor Authentication (MFA) Delete on the S3 bucket and ensure that only authorized users can access the logs by configuring the bucket policies.

Q101. An online shopping platform is hosted on an Auto Scaling group of Spot EC2 instances and uses Amazon Aurora PostgreSQL as its database. There is

a requirement to optimize your database workloads in your cluster where you have to direct the write operations of the production traffic to your high-capacity instances and point the reporting queries sent by your internal staff to the low-capacity instances. Which is the most suitable configuration for your application as well as your Aurora database cluster to achieve this requirement?

A. In your application, use the instance endpoint of your Aurora database to handle the incoming production traffic and use the cluster endpoint to handle reporting queries.

B. Configure your application to use the reader endpoint for both production traffic and reporting queries, which will enable your Aurora database to automatically perform load- balancing among all the Aurora Replicas.

C. Do nothing since by default, Aurora will automatically direct the production traffic to your high-capacity instances and the reporting queries to your low-capacity instances.

D. Create a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries.

Q102. A company is using Amazon S3 to store frequently accessed data. When an object is created or deleted, the S3 bucket will send an event notification to the Amazon SQS queue. A solutions architect needs to create a solution that will notify the development and operations team about the created or deleted objects.

Which of the following would satisfy this requirement?

A. Create a new Amazon SNS FIFO topic for the other team. Grant Amazon S3 permission to send the notification to the second SNS topic.

B. Set up another Amazon SQS queue for the other team. Grant Amazon S3 permission to send a notification to the second SQS queue.

C. Set up an Amazon SNS topic and configure two Amazon SQS queues to poll the SNS topic.

Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic.

D. Create an Amazon SNS topic and configure two Amazon SQS queues to subscribe to the topic. Grant Amazon S3 permission to send notifications to Amazon SNS and update the bucket to use the new SNS topic.

Q103. A company plans to launch an Amazon EC2 instance in a private subnet for its internal corporate web portal. For security purposes, the EC2 instance must send data to Amazon DynamoDB and Amazon S3 via private endpoints that don't pass through the public Internet.

Which of the following can meet the above requirements?

A. Use AWS VPN CloudHub to route all access to S3 and DynamoDB via private endpoints.

B. Use AWS Transit Gateway to route all access to S3 and DynamoDB via private endpoints.

C. Use AWS Direct Connect to route all access to S3 and DynamoDB via

private endpoints.

D. Use VPC endpoints to route all access to S3 and DynamoDB via private endpoints.

Q104. A company hosted a web application in an Auto Scaling group of EC2 instances. The IT manager is concerned about the over-provisioning of the resources that can cause higher operating costs. A Solutions Architect has been instructed to create a cost-effective solution without affecting the performance of the application.

Which dynamic scaling policy should be used to satisfy this requirement?

- A. Use simple scaling.
- B. Use suspend and resume scaling.
- C. Use scheduled scaling.
- D. Use target tracking scaling.

Q105. A company needs to design an online analytics application that uses Redshift Cluster for its data warehouse. Which of the following services allows them to monitor all API calls in Redshift instance and can also provide secured data for auditing and compliance purposes?

- A. AWS CloudTrail
- B. Amazon CloudWatch
- C. AWS X-Ray



## D. Amazon Redshift Spectrum

Q106. A startup is using Amazon RDS to store data from a web application. Most of the time, the application has low user activity but it receives bursts of traffic within seconds whenever there is a new product announcement. The Solutions Architect needs to create a solution that will allow users around the globe to access the data using an API.

What should the Solutions Architect do meet the above requirement?

- A. Create an API using Amazon API Gateway and use the Amazon ECS cluster with Service Auto Scaling to handle the bursts of traffic in seconds.
- B. Create an API using Amazon API Gateway and use Amazon Elastic Beanstalk with Auto Scaling to handle the bursts of traffic in seconds.
- C. Create an API using Amazon API Gateway and use an Auto Scaling group of Amazon EC2 instances to handle the bursts of traffic in seconds.
- D. Create an API using Amazon API Gateway and use AWS Lambda to handle the bursts of traffic in seconds.

Q107. A company has a cloud architecture that is composed of Linux and Windows EC2 instances that process high volumes of financial data 24 hours a day, 7 days a week. To ensure high availability of the systems, the Solutions Architect needs to create a solution that allows them to monitor the memory and disk utilization metrics of all the instances.

Which of the following is the most suitable monitoring solution to implement?

A. Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all the EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard.

B. Use Amazon Inspector and install the Inspector agent to all EC2 instances.

C. Install the CloudWatch agent to all the EC2 instances that gathers the memory and disk utilization data.

View the custom metrics in the Amazon CloudWatch console.

D. Use the default CloudWatch configuration to EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all the EC2 instances.

Q108. A company is in the process of migrating their applications to AWS. One of their systems requires a database that can scale globally and handle frequent schema changes. The application should not have any downtime or performance issues whenever there is a schema change in the database. It should also provide a low latency response to high-traffic queries.

Which is the most suitable database solution to use to achieve this requirement?

A. Redshift

B. Amazon DynamoDB

C. An Amazon RDS instance in Multi-AZ Deployments configuration

D. An Amazon Aurora database with Read Replicas

Q109. A company is using a combination of API Gateway and Lambda for the web services of the online web portal that is being accessed by hundreds of thousands of clients each day. They will be announcing a new revolutionary product and it is expected that the web portal will receive a massive number of visitors all around the globe.

How can you protect the backend systems and applications from traffic spikes?

- A. Use throttling limits in API Gateway
- B. API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything.
- C. Manually upgrade the EC2 instances being used by API Gateway
- D. Deploy Multi-AZ in API Gateway with Read Replica

Q110. A company is designing a banking portal that uses Amazon ElastiCache for Redis as its distributed session management component. Since the other Cloud Engineers in your department have access to your ElastiCache cluster, you have to secure the session data in the portal by requiring them to enter a password before they are granted permission to execute Redis commands. As the Solutions Architect, which of the following should you do to meet the above requirement?

- A. Authenticate the users using Redis AUTH by creating a new Redis Cluster

with both the `--transit-encryption-enabled` and `--auth-token-enabled` parameters enabled.

B. Set up a Redis replication group and enable the `AtRestEncryptionEnabled` parameter.

C. Set up an IAM Policy and MFA which requires the Cloud Engineers to enter their IAM credentials and token before they can access the ElastiCache cluster.

D. Enable the in-transit encryption for Redis replication groups.

Q111. A company plans to host a web application in an Auto Scaling group of Amazon EC2 instances. The application will be used globally by users to upload and store several types of files. Based on user trends, files that are older than 2 years must be stored in a different storage class. The Solutions Architect of the company needs to create a cost-effective and scalable solution to store the old files yet still provide durability and high availability.

Which of the following approach can be used to fulfill this requirement? (Select TWO.)

A. Use Amazon EBS volumes to store the files. Configure the Amazon Data Lifecycle Manager (DLM) to schedule snapshots of the volumes after 2 years.

B. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Glacier after 2 years.

C. Use a RAID 0 storage configuration that stripes multiple Amazon EBS volumes together to store the files. Configure the Amazon Data Lifecycle

Manager (DLM) to schedule snapshots of the volumes after 2 years.

D. Use Amazon S3 and create a lifecycle policy that will move the objects to Amazon S3 Standard-IA after 2 years.

E. Use Amazon EFS and create a lifecycle policy that will move the objects to Amazon EFS-IA after 2 years.

Q112. An online medical system hosted in AWS stores sensitive Personally Identifiable Information (PII) of the users in an Amazon S3 bucket. Both the master keys and the unencrypted data should never be sent to AWS to comply with the strict compliance and regulatory requirements of the company. Which S3 encryption technique should the Architect use?

A. Use S3 client-side encryption with a client-side master key.

B. Use S3 client-side encryption with a KMS-managed customer master key.

C. Use S3 server-side encryption with a KMS managed key.

D. Use S3 server-side encryption with customer provided key.

Q113. An application consists of multiple EC2 instances in private subnets in different availability zones. The application uses a single NAT Gateway for downloading software patches from the Internet to the instances.

There is a

requirement to protect the application from a single point of failure when the NAT Gateway encounters a failure or if its availability zone goes down.

How should the Solutions Architect redesign the architecture to be more highly available and cost-effective

A. Create three NAT Gateways in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone.

B. Create a NAT Gateway in each availability zone. Configure the route table in each private subnet to ensure that instances use the NAT Gateway in the same availability zone

C. Create two NAT Gateways in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.

D. Create a NAT Gateway in each availability zone. Configure the route table in each public subnet to ensure that instances use the NAT Gateway in the same availability zone.

Q114. A company collects atmospheric data such as temperature, air pressure, and humidity from different countries. Each site location is equipped with various weather instruments and a high-speed Internet connection. The average collected data in each location is around 500 GB and will be analyzed by a weather forecasting application hosted in Northern Virginia. As the Solutions Architect, you need to aggregate all the data in the fastest way.

Which of the following options can satisfy the given requirement?

- A. Set up a Site-to-Site VPN connection.
- B. Enable Transfer Acceleration in the destination bucket and upload the collected data using Multipart Upload.
- C. Upload the data to the closest S3 bucket. Set up a cross-region replication and copy the objects to the destination bucket.
- D. Use AWS Snowball Edge to transfer large amounts of data.

Q115. A company plans to build a data analytics application in AWS which will be deployed in an Auto Scaling group of On-Demand EC2 instances and a MongoDB database. It is expected that the database will have highthroughput workloads performing small, random I/O operations. As the Solutions Architect, you are required to properly set up and launch the required resources in AWS. Which of the following is the most suitable EBS type to use for your database?

- A. General Purpose SSD (gp2)
- B. Cold HDD (sc1)
- C. Throughput Optimized HDD (st1)
- D. Provisioned IOPS SSD (io1)

Answer D

Q116. A global IT company with offices around the world has multiple AWS accounts. To improve efficiency and drive costs down, the Chief Information

Officer (CIO) wants to set up a solution that centrally manages their AWS resources. This will allow them to procure AWS resources centrally and share resources such as AWS Transit Gateways, AWS License Manager configurations, or Amazon Route 53 Resolver rules across their various accounts.

As the Solutions Architect, which combination of options should you implement in this scenario? (Select TWO.)

- A. Use the AWS Identity and Access Management service to set up cross-account access that will easily and securely share your resources with your AWS accounts.
- B. Consolidate all of the company's accounts using AWS ParallelCluster.
- C. Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.
- D. Use AWS Control Tower to easily and securely share your resources with your AWS accounts.
- E. Consolidate all of the company's accounts using AWS Organizations.

Q117. A tech company that you are working for has undertaken a Total Cost Of Ownership (TCO) analysis evaluating the use of Amazon S3 versus acquiring more storage hardware. The result was that all 1200 employees would be granted access to use Amazon S3 for the storage of their personal documents. Which of the following will you need to consider so you can set up a solution



that incorporates a single sign-on feature from your corporate AD or LDAP directory and also restricts access for each individual user to a designated user folder in an S3 bucket? (Select TWO.)

- A. Set up a matching IAM user for each of the 1200 users in your corporate directory that needs access to a folder in the S3 bucket.
- B. Configure an IAM role and an IAM Policy to access the bucket.
- C. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.
- D. Map each individual user to a designated user folder in S3 using Amazon WorkDocs to access their personal documents.
- E. Set up a Federation proxy or an Identity provider, and use AWS Security Token Service to generate temporary tokens.

Q118. There are a lot of outages in the Availability Zone of your RDS database instance to the point that you have lost access to the database. What could you do to prevent losing access to your database in case that this event happens again?

- A. Make a snapshot of the database
- B. Increase the database instance size
- C. Create a read replica
- D. Enabled Multi-AZ failover

Q119. A cryptocurrency trading platform is using an API built in AWS Lambda and API Gateway. Due to the recent news and rumors about the upcoming price surge of Bitcoin, Ethereum and other cryptocurrencies, it is expected that the trading platform would have a significant increase in site visitors and new users in the coming days ahead.

In this scenario, how can you protect the backend systems of the platform from traffic spikes?

- A. Move the Lambda function in a VPC.
- B. Enable throttling limits and result caching in API Gateway.
- C. Use CloudFront in front of the API Gateway to act as a cache.
- D. Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling.

Q120. A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances that use Amazon Aurora as its database. Currently, the system stores the file documents that the users upload in one of the attached EBS Volumes. Your manager noticed that the system performance is quite slow and he has instructed you to improve the architecture of the system. In this scenario, what will you do to implement a scalable, high-available POSIX-compliant shared file system?

- A. Create an S3 bucket and use this as the storage for the CMS
- B. Upgrading your existing EBS volumes to Provisioned IOPS SSD Volumes

C. Use ElastiCache

D. Use EFS

Q121. A company has a hybrid cloud architecture that connects their on-premises data center and cloud infrastructure in AWS. They require a durable storage backup for their corporate documents stored on-premises and a local cache that provides low latency access to their recently accessed data to reduce data egress charges. The documents must be stored to and retrieved from AWS via the Server Message Block (SMB) protocol. These files must immediately be accessible within minutes for six months and archived for another decade to meet the data compliance.

Which of the following is the best and most cost-effective approach to implement in this scenario?

A. Launch a new file gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the file gateway and set up a lifecycle policy to move the data into Glacier for data archival.

B. Use AWS Snowmobile to migrate all of the files from the on-premises network. Upload the documents to an S3 bucket and set up a lifecycle policy to move the data into Glacier for archival.

C. Establish a Direct Connect connection to integrate your on-premises network to your VPC.

Upload the documents on Amazon EBS Volumes and use a lifecycle policy to

automatically move the EBS snapshots to an S3 bucket, and then later to Glacier for archival.

D. Launch a new tape gateway that connects to your on-premises data center using AWS Storage Gateway. Upload the documents to the tape gateway and set up a lifecycle policy to move the data into Glacier for archival.

Q122. A web application is using CloudFront to distribute their images, videos, and other static contents stored in their S3 bucket to its users around the world. The company has recently introduced a new member-only access to some of its high quality media files. There is a requirement to provide access to multiple private media files only to their paying subscribers without having to change their current URLs. Which of the following is the most suitable solution that you should implement to satisfy this requirement?

A. Configure your CloudFront distribution to use Match Viewer as its Origin Protocol Policy which will automatically match the user request. This will allow access to the private content if the request is a paying member and deny it if it is not a member.

B. Create a Signed URL with a custom policy which only allows the members to see the private files.

C. Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members.

D. Use Signed Cookies to control who can access the private files in your

CloudFront distribution by modifying your application to determine whether a user should have access to your content. For members, send the required Set-Cookie headers to the viewer which will unlock the content only to them.

Q123. A company is hosting its web application in an Auto Scaling group of EC2 instances behind an Application Load Balancer. Recently, the Solutions Architect identified a series of SQL injection attempts and cross-site scripting attacks to the application, which had adversely affected their production data. Which of the following should the Architect implement to mitigate this kind of attack?

- A. Using AWS Firewall Manager, set up security rules that block SQL injection and cross-site scripting attacks. Associate the rules to the Application Load Balancer.
- B. Use Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application.
- C. Set up security rules that block SQL injection and cross-site scripting attacks in AWS Web Application Firewall (WAF). Associate the rules to the Application Load Balancer.
- D. Block all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List.

Q124. An insurance company utilizes SAP HANA for its day-to-day ERP

operations. Since they can't migrate this database due to customer preferences, they need to integrate it with the current AWS workload in the VPC in which they are required to establish a site-to-site VPN connection. What needs to be configured outside of the VPC for them to have a successful site-to-site VPN connection?

- A. An EIP to the Virtual Private Gateway
- B. The main route table in your VPC to route traffic through a NAT instance
- C. A dedicated NAT instance in a public subnet
- D. An Internet-routable IP address (static) of the customer gateway's external interface for the on-premises network

Q125. A company has a data analytics application that updates a real-time, foreign exchange dashboard and another separate application that archives data to Amazon Redshift. Both applications are configured to consume data from the same stream concurrently and independently by using Amazon Kinesis Data Streams. However, they noticed that there are a lot of occurrences where a shard iterator expires unexpectedly. Upon checking, they found out that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

Which of the following is the most suitable solution to rectify this issue?

- A. Use Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream.

- B. Upgrade the storage capacity of the DynamoDB table.
- C. Increase the write capacity assigned to the shard table.
- D. Enable In-Memory Acceleration with DynamoDB Accelerator (DAX).

Q126. A web application, which is used by your clients around the world, is hosted in an Auto Scaling group of EC2 instances behind a Classic Load Balancer. You need to secure your application by allowing multiple domains to serve SSL traffic over the same IP address.

Which of the following should you do to meet the above requirement?

- A. Use an Elastic IP and upload multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager.
- B. Use Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic.
- C. Generate an SSL certificate with AWS Certificate Manager and create a CloudFront web distribution. Associate the certificate with your web distribution and enable the support for Server Name Indication (SNI).
- D. It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS

Q127. A company has two On-Demand EC2 instances inside the Virtual Private Cloud in the same Availability Zone but are deployed to different subnets. One EC2 instance is running a database and the other EC2 instance a web

application that connects with the database. You need to ensure that these two instances can

communicate with each other for the system to work properly. What are the things you have to check so that these EC2 instances can communicate inside the VPC? (Select TWO.)

- A. Ensure that the EC2 instances are in the same Placement Group.
- B. Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.
- C. Check if both instances are the same instance class.
- D. Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate.
- E. Check the Network ACL if it allows communication between the two subnets.

Q128. As part of the Business Continuity Plan of your company, your IT Director instructed you to set up an automated backup of all of the EBS Volumes for your EC2 instances as soon as possible. What is the fastest and most cost-effective solution to automatically back up all of your EBS Volumes?

- A. Use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots.
- B. Set your Amazon Storage Gateway with EBS volumes as the data source and store the backups in your on-premises servers through the storage gateway.



C. Use an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes.

D. For an automated solution, create a scheduled job that calls the "create-snapshot" command via the AWS CLI to take a snapshot of production EBS volumes periodically.

Q129.A website that consists of HTML, CSS, and other client-side Javascript will be hosted on the AWS environment. Several high-resolution images will be displayed on the webpage. The website and the photos should have the optimal loading response times as possible, and should also be able to scale to high request rates.

Which of the following architectures can provide the most cost-effective and fastest loading experience?

A. Launch an Auto Scaling Group using an AMI that has a pre-configured Apache web server, then configure the scaling policy accordingly. Store the images in an Elastic Block Store. Then, point your instance's endpoint to AWS Global Accelerator.

B. Create a Nginx web server in an Amazon LightSail instance to host the HTML, CSS, and Javascript files then enable caching. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to your end-users.

C. Upload the HTML, CSS, Javascript, and the images in a single bucket. Then

enable website hosting.

Create a CloudFront distribution and point the domain on the S3 website endpoint.

D. Create a Nginx web server in an EC2 instance to host the HTML, CSS, and Javascript files then enable caching. Upload the images in an S3 bucket. Use CloudFront as a CDN to deliver the images closer to your end-users.

Q130. You have built a web application that checks for new items in an S3 bucket once every hour. If new items exist, a message is added to an SQS queue. You have a fleet of EC2 instances which retrieve messages from the SQS queue, process the file, and finally, send you and the user an email confirmation that the item has been successfully processed. Your officemate uploaded one test file to the S3 bucket and after a couple of hours, you noticed that you and your officemate have 50 emails from your application with the same message. Which of the following is most likely the root cause why the application has sent you and the user multiple emails?

A. There is a bug in the application.

B. By default, SQS automatically deletes the messages that were processed by the consumers. It might be possible that your officemate has submitted the request 50 times which is why you received a lot of emails.

C. The `sqsSendMessage` attribute of the SQS queue is configured to 50

D. Your application does not issue a delete command to the SQS queue after

processing the message, which is why this message went back to the queue and was processed multiple times.

Q131. A Network Architect developed a food ordering application. The Architect needs to retrieve the instance ID, public keys, and public IP address of the EC2 server made for tagging and grouping the attributes into the internal application running on-premises.

Which of the following options fulfills this requirement?

- A. Amazon Machine Image
- B. Instance user data
- C. Resource tags
- D. Instance metadata

Q132. A DevOps Engineer is required to design a cloud architecture in AWS. The Engineer is planning to develop a highly available and fault-tolerant architecture that is composed of an Elastic Load Balancer and an Auto Scaling group of EC2 instances deployed across multiple Availability Zones. This will be used by an online accounting application that requires path-based routing, host-based routing, and bi-directional communication channels using WebSockets.

Which is the most suitable type of Elastic Load Balancer that will satisfy the given requirement?

- A. Gateway Load Balancer
- B. Network Load Balancer
- C. Application Load Balancer
- D. Classic Load Balancer

Q133. A software company has resources hosted in AWS and on-premises servers. You have been requested to create a decoupled architecture for applications which make use of both resources. Which of the following options are valid? (Select TWO.)

- A. Use SWF to utilize both on-premises servers and EC2 instances for your decoupled application
- B. Use SQS to utilize both on-premises servers and EC2 instances for your decoupled application
- C. Use RDS to utilize both on-premises servers and EC2 instances for your decoupled application
- D. Use DynamoDB to utilize both on-premises servers and EC2 instances for your decoupled application
- E. Use VPC peering to connect both on-premises servers and EC2 instances for your decoupled application

Q134. A company developed a meal planning application that provides meal recommendations for the week as well as the food consumption of the users.

The application resides on an EC2 instance which requires access to various AWS services for its day-to-day operations. Which of the following is the best way to allow the EC2 instance to access the S3 bucket and other AWS services?

- A. Add the API Credentials in the Security Group and assign it to the EC2 instance.
- B. Store the API credentials in a bastion host.
- C. Create a role in IAM and assign it to the EC2 instance.
- D. Store the API credentials in the EC2 instance.

Q135. An organization stores and manages financial records of various companies in its on-premises data center, which is almost out of space. The management decided to move all of their existing records to a cloud storage service. All future financial records will also be stored in the cloud. For additional security, all records must be prevented from being deleted or overwritten. Which of the following should you do to meet the above requirement?

- A. Use AWS DataSync to move the data. Store all of your data in Amazon EFS and enable object lock.
- B. Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon S3 and enable object lock.
- C. Use AWS Storage Gateway to establish hybrid cloud storage. Store all of your data in Amazon EBS and enable object lock.

D. Use AWS DataSync to move the data. Store all of your data in Amazon S3 and enable object lock.

Q136. A Solutions Architect created a new Standard-class S3 bucket to store financial reports that are not frequently accessed but should immediately be available when an auditor requests them. To save costs, the Architect changed the storage class of the S3 bucket from Standard to Infrequent Access storage class. In Amazon S3 Standard - Infrequent Access storage class, which of the following statements are true? (Select TWO.)

- A. Ideal to use for data archiving.
- B. It is designed for data that is accessed less frequently.
- C. It provides high latency and low throughput performance
- D. It is designed for data that requires rapid access when needed.
- E. It automatically moves data to the most cost-effective access tier without any operational overhead.

Q137. A media company is setting up an ECS batch architecture for its image processing application. It will be hosted in an Amazon ECS Cluster with two ECS tasks that will handle image uploads from the users and image processing. The first ECS task will process the user requests, store the image in an S3 input bucket, and push a message to a queue. The second task reads from the queue, parses the message containing the object name, and then downloads

the object. Once the image is processed and transformed, it will upload the objects to the S3 output bucket. To complete the architecture, the Solutions Architect must create a queue and the necessary IAM permissions for the ECS tasks.

Which of the following should the Architect do next?

A. Launch a new Amazon Kinesis Data Firehose and configure the second ECS task to read from it.

Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Kinesis Data Firehose. Specify the ARN of the IAM Role in the (taskDefinitionArn) field of the task definition.

B. Launch a new Amazon AppStream 2.0 queue and configure the second ECS task to read from it.

Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and AppStream 2.0 queue. Declare the IAM Role (taskRoleArn) in the task definition.

C. a new Amazon SQS queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and SQS queue. Declare the IAM Role (taskRoleArn) in the task definition.

D. a new Amazon MQ queue and configure the second ECS task to read from it. Create an IAM role that the ECS tasks can assume in order to get access to the S3 buckets and Amazon MQ queue. Set the (EnableTaskIAMRole) option

to true in the task definition.

Q138. A company has a top priority requirement to monitor a few database metrics and then afterward, send email notifications to the Operations team in case there is an issue. Which AWS services can accomplish this requirement?

(Select TWO.)

- A. Amazon EC2 Instance with a running Berkeley Internet Name Domain (BIND) Server.
- B. Amazon CloudWatch
- C. Simple Notification Service (SNS)
- D. Amazon Simple Email Service
- E. Simple Queue Service (SQS)

Q139. A media company has two VPCs: VPC-1 and VPC-2 with peering connection between each other. VPC-1 only contains private subnets while VPC-2 only contains public subnets. The company uses a single AWS Direct Connect connection and a virtual interface to connect their on-premises network with VPC-1. Which of the following options increase the fault tolerance of the connection to VPC-1? (Select TWO.)

- A. Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- B. Establish another AWS Direct Connect connection and private virtual



interface in the same AWS region as VPC-1.

C. Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.

D. Establish a hardware VPN over the Internet between VPC-1 and the on-premises network.

E. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

Q140. A Solutions Architect of a multinational gaming company develops video games for PS4, Xbox One, and Nintendo Switch consoles, plus a number of mobile games for Android and iOS. Due to the wide range of their products and services, the architect proposed that they use API Gateway. What are the key features of API Gateway that the architect can tell to the client? (Select TWO.)

A. Enables you to run applications requiring high levels of inter-node communications at scale on AWS through its custom-built operating system (OS) bypass hardware interface.

B. It automatically provides a query language for your APIs similar to GraphQL.

C. You pay only for the API calls you receive and the amount of data transferred out.

D. Provides you with static anycast IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions.

E. you to build RESTful APIs and WebSocket APIs that are optimized for

serverless workloads.

Answer CE

Q141. A company has multiple VPCs with IPv6 enabled for its suite of web applications. The Solutions Architect tried to deploy a new Amazon EC2 instance but she received an error saying that there is no IP address available on the subnet.

How should the Solutions Architect resolve this problem?

- A. Set up a new IPv6-only subnet with a large CIDR range. Associate the new subnet with the VPC then launch the instance.
- B. Set up a new IPv4 subnet with a larger CIDR range. Associate the new subnet with the VPC and then launch the instance.
- C. Disable the IPv4 support in the VPC and use the available IPv6 addresses.
- D. Ensure that the VPC has IPv6 CIDRs only. Remove any IPv4 CIDRs associated with the VPC.

Q142. An insurance company plans to implement a message filtering feature in their web application. To implement this solution, they need to create separate Amazon SQS queues for each type of quote request.

The entire message processing should not exceed 24 hours.

As the Solutions Architect of the company, which of the following should you do to meet the above requirement?

- A. Create multiple Amazon SNS topics and configure the Amazon SQS queues

to subscribe to the SNS topics. Publish the message to the designated SQS queue based on the quote request type.

B. Create a data stream in Amazon Kinesis Data Streams. Use the Amazon Kinesis Client Library to deliver all the records to the designated SQS queues based on the quote request type.

C. Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic.

Publish the same messages to all SQS queues. Filter the messages in each queue based on the quote request type.

com

com

D. Create one Amazon SNS topic and configure the Amazon SQS queues to subscribe to the SNS topic.

Set the filter policies in the SNS subscriptions to publish the message to the designated SQS queue based on its quote request type.

Q143. A music publishing company is building a multitier web application that requires a key-value store which will save the document models. Each model is composed of band ID, album ID, song ID, composer ID, lyrics, and other data. The web tier will be hosted in an Amazon ECS cluster with AWS Fargate launch type. Which of the following is the MOST suitable setup for the database-tier?

A. Launch an Amazon Aurora Serverless database.

- B. Launch an Amazon RDS database with Read Replicas.
- C. Launch a DynamoDB table.
- D. Use Amazon WorkDocs to store the document models.

Q144. An application is hosted in AWS Fargate and uses RDS database in Multi-AZ Deployments configuration with several Read Replicas. A Solutions Architect was instructed to ensure that all of their database credentials, API keys, and other secrets are encrypted and rotated on a regular basis to improve data security. The application should also use the latest version of the encrypted credentials when connecting to the RDS database.

Which of the following is the MOST appropriate solution to secure the credentials?

- A. Store the database credentials, API keys, and other secrets to Systems Manager Parameter Store each with a SecureString data type. The credentials are automatically rotated by default.
- B. Store the database credentials, API keys, and other secrets in AWS KMS.
- C. Store the database credentials, API keys, and other secrets to AWS ACM.
- D. Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets.

Enable automatic rotation for all of the credentials.

Q145. An advertising company is currently working on a proof of concept

project that automatically provides SEO analytics for its clients. Your company has a VPC in AWS that operates in a dual-stack mode in which IPv4 and IPv6 communication is allowed. You deployed the application to an Auto Scaling group of EC2 instances with an Application Load Balancer in front that evenly distributes the incoming traffic. You are ready to go live but you need to point your domain name (tutorialsdojo.com) to the Application Load Balancer.

In Route 53, which record types will you use to point the DNS name of the Application Load Balancer? (Select TWO.)

- A. Alias with a type "A" record set
- B. Non-Alias with a type "A" record set
- C. Alias with a type "AAAA" record set
- D. Alias with a type "CNAME" record set
- E. Alias with a type of "MX" record set

Q146. A Solutions Architect is working for an online hotel booking firm with terabytes of customer data coming from the websites and applications. There is an annual corporate meeting where the Architect needs to present the booking behavior and acquire new insights from the customers' data. The Architect is looking for a service to perform super-fast analytics on massive data sets in near real-time. Which of the following services gives the Architect the ability to store huge amounts of data and perform quick and flexible queries on it?

- A. Amazon DynamoDB
- B. Amazon RDS
- C. Amazon Redshift
- D. Amazon ElastiCache

Q147. One of your EC2 instances is reporting an unhealthy system status check. The operations team is looking for an easier way to monitor and repair these instances instead of fixing them manually. How will you automate the monitoring and repair of the system status check failure in an AWS environment?

- A. Write a python script that queries the EC2 API for each instance status check
- B. Write a shell script that periodically shuts down and starts instances based on certain stats.
- C. and implement a third party monitoring tool.
- D. Create CloudWatch alarms that stop and start the instance based on status check alarms.

Q148. A Solutions Architect needs to set up a bastion host in Amazon VPC. It should only be accessed from the corporate data center via SSH. What is the best way to achieve this?

- A. Create a small EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key

(.pem) file to connect to the bastion host.

B. Create a large EC2 instance with a security group which only allows access on port 22 using your own preconfigured password.

C. Create a small EC2 instance with a security group which only allows access on port 22 using your own preconfigured password.

D. Create a large EC2 instance with a security group which only allows access on port 22 via the IP address of the corporate data center. Use a private key (.pem) file to connect to the bastion host.

Q149. A company has a cryptocurrency exchange portal that is hosted in an Auto Scaling group of EC2 instances behind an Application Load Balancer and is deployed across multiple AWS regions. The users can be found all around the globe, but the majority are from Japan and Sweden. Because of the compliance requirements in these two locations, you want the Japanese users to connect to the servers in the ap- northeast-1 Asia Pacific (Tokyo) region, while the Swedish users should be connected to the servers in the euwest-1 EU (Ireland) region.

Which of the following services would allow you to easily fulfill this requirement?

A. Use Route 53 Weighted Routing policy.

B. Use Route 53 Geolocation Routing policy.

C. Set up a new CloudFront web distribution with the geo-restriction feature enabled.

D. Set up an Application Load Balancers that will automatically route the traffic to the proper AWS region.

Q150. An Intelligence Agency developed a missile tracking application that is hosted on both development and production AWS accounts. The Intelligence agency's junior developer only has access to the development account. She has received security clearance to access the agency's production account but the access is only temporary and only write access to EC2 and S3 is allowed. Which of the following allows you to issue short-lived access tokens that act as temporary security credentials to allow access to your AWS resources?

- A. All of the given options are correct.
- B. Use AWS STS
- C. Use AWS SSO
- D. Use AWS Cognito to issue JSON Web Tokens (JWT)

Q151. A digital media company shares static content to its premium users around the world and also to their partners who syndicate their media files. The company is looking for ways to reduce its server costs and securely deliver their data to their customers globally with low latency. Which combination of services should be used to provide the MOST suitable and cost-effective architecture? (Select TWO.)

- A. Amazon S3



- B. AWS Global Accelerator
- C. AWS Lambda
- D. Amazon CloudFront
- E. AWS Fargate

Q152. A Solutions Architect is building a cloud infrastructure where EC2 instances require access to various AWS services such as S3 and Redshift. The Architect will also need to provide access to system administrators so they can deploy and test their changes.

Which configuration should be used to ensure that the access to the resources is secured and not compromised? (Select TWO.)

- A. Store the AWS Access Keys in ACM.
- B. Store the AWS Access Keys in the EC2 instance.
- C. Enable Multi-Factor Authentication.
- D. Assign an IAM role to the Amazon EC2 instance.
- E. Assign an IAM user for each Amazon EC2 Instance.

Q153. A company plans to migrate all of their applications to AWS. The Solutions Architect suggested to store all the data to EBS volumes. The Chief Technical Officer is worried that EBS volumes are not appropriate for the existing workloads due to compliance requirements, downtime scenarios, and IOPS performance. Which of the following are valid points in proving that EBS

is the best service to use for migration? (Select TWO.)

- A. EBS volumes can be attached to any EC2 Instance in any Availability Zone.
- B. When you create an EBS volume in an Availability Zone, it is automatically replicated on a separate AWS region to prevent data loss due to a failure of any single hardware component.
- C. An EBS volume is off-instance storage that can persist independently from the life of an instance.
- D. EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.
- E. Amazon EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to Amazon RDS, where it is stored redundantly in multiple Availability Zones

Q154. A company needs to assess and audit all the configurations in their AWS account. It must enforce strict compliance by tracking all configuration changes made to any of its Amazon S3 buckets. Publicly accessible S3 buckets should also be identified automatically to avoid data breaches. Which of the following options will meet this requirement?

- A. Use AWS CloudTrail and review the event history of your AWS account.
- B. Use AWS Trusted Advisor to analyze your AWS environment.
- C. Use AWS IAM to generate a credential report.

D. Use AWS Config to set up a rule in your AWS account.

Q155. A Data Engineer is working for a litigation firm for their case history application. The engineer needs to keep track of all the cases that the firm has handled. The static assets like .jpg, .png, and .pdf files are stored in S3 for cost efficiency and high durability. As these files are critical to the business, the engineer wants to keep track of what's happening in the S3 bucket. The engineer found out that S3 has an event notification whenever a delete or write operation happens within the S3 bucket. What are the possible Event Notification destinations available for S3 buckets? (Select TWO.)

A. SQS

B. SWF

C. SES

D. Lambda function

E. Kinesis

Q156. A company is building an internal application that serves as a repository for images uploaded by a couple of users. Whenever a user uploads an image, it would be sent to Kinesis Data Streams for processing before it is stored in an S3 bucket. If the upload was successful, the application will return a prompt informing the user that the operation was successful. The entire processing typically takes about 5 minutes to finish. Which of the following options will allow you to asynchronously process the request to the application from upload

request to Kinesis, S3, and return a reply in the most cost-effective manner?

- A. Replace the Kinesis Data Streams with an Amazon SQS queue. Create a Lambda function that will asynchronously process the requests.
- B. Use a combination of SQS to queue the requests and then asynchronously process them using On-Demand EC2 Instances.
- C. Use a combination of Lambda and Step Functions to orchestrate service components and asynchronously process the requests.
- D. Use a combination of SNS to buffer the requests and then asynchronously process them using On-Demand EC2 Instances.

Q157. A media company hosts large volumes of archive data that are about 250 TB in size on their internal servers. They have decided to move these data to S3 because of its durability and redundancy. The company currently has a 100 Mbps dedicated line connecting their head office to the Internet. Which of the following is the FASTEST and the MOST cost-effective way to import all these data to Amazon S3?

- A. Upload it directly to S3
- B. Use AWS Snowmobile to transfer the data over to S3.
- C. Establish an AWS Direct Connect connection then transfer the data over to S3.
- D. Order multiple AWS Snowball devices to upload the files to Amazon S3.

Q158. A company is working with a government agency to improve traffic planning and maintenance of roadways to prevent accidents. The proposed solution is to manage the traffic infrastructure in real-time, alert traffic engineers and emergency response teams when problems are detected, and automatically change traffic signals to get emergency personnel to accident scenes faster by using sensors and smart devices. Which AWS service will allow the developers of the agency to connect the smart devices to the cloud-based applications?

- A. AWS Elastic Beanstalk
- B. AWS CloudFormation
- C. Amazon Elastic Container Service
- D. AWS IoT Core

Q159. A commercial bank has a forex trading application. They created an Auto Scaling group of EC2 instances that allow the bank to cope with the current traffic and achieve cost-efficiency. They want the Auto Scaling group to behave in such a way that it will follow a predefined set of parameters before it scales down the number of EC2 instances, which protects the system from unintended slowdown or unavailability. Which of the following statements are true regarding the cooldown period? (Select TWO.)

- A. Its default value is 300 seconds.
- B. It ensures that the Auto Scaling group does not launch or terminate additional

EC2 instances before the previous scaling activity takes effect.

C. It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.

D. Its default value is 600 seconds.

E. It ensures that before the Auto Scaling group scales out, the EC2 instances have ample time to cooldown.

Q160. An organization needs to control the access for several S3 buckets. They plan to use a gateway endpoint to allow access to trusted buckets.

Which of the following could help you achieve this requirement?

A. Generate an endpoint policy for trusted S3 buckets.

B. Generate a bucket policy for trusted VPCs.

C. Generate an endpoint policy for trusted VPCs.

D. Generate a bucket policy for trusted S3 buckets.

Q161. A company has an enterprise web application hosted on Amazon ECS Docker containers that use an Amazon FSx for Lustre filesystem for its high-performance computing workloads. A warm standby environment is running in another AWS region for disaster recovery. A Solutions Architect was assigned to design a system that will automatically route the live traffic to the disaster recovery (DR) environment only in the event that the primary application stack experiences an outage. What should the Architect do to satisfy this

requirement?

A. Set up a CloudWatch Events rule to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record.

B. Set up a Weighted routing policy configuration in Route 53 by adding health checks on both the primary stack and the DR environment. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks.

Enable the Evaluate Target Health option by setting it to Yes.

C. Set up a failover routing policy configuration in Route 53 by adding a health check on the primary service endpoint. Configure Route 53 to direct the DNS queries to the secondary record when the primary resource is unhealthy. Configure the network access control list and the route table to allow Route 53 to send requests to the endpoints specified in the health checks. Enable the Evaluate Target Health option by setting it to Yes.

D. Set up a CloudWatch Alarm to monitor the primary Route 53 DNS endpoint and create a custom Lambda function. Execute the ChangeResourceRecordSets API call using the function to initiate the failover to the secondary DNS record.

Q162. A Solutions Architect is working for a company that uses Chef

Configuration management in their data center. She needs to leverage their existing Chef recipes in AWS.

Which of the following services should she use?

- A. AWS CloudFormation
- B. AWS OpsWorks
- C. Amazon Simple Workflow Service
- D. AWS Elastic Beanstalk

Q163. An organization is currently using a tape backup solution to store its application data on-premises. They plan to use a cloud storage service to preserve the backup data for up to 10 years that may be accessed about once or twice a year.

Which of the following is the most cost-effective option to implement this solution?

- A. Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier Deep Archive.
- B. Order an AWS Snowball Edge appliance to import the backup directly to Amazon S3 Glacier.
- C. Use AWS Storage Gateway to backup the data directly to Amazon S3 Glacier.
- D. Use Amazon S3 to store the backup data and add a lifecycle rule to transition the current version to Amazon S3 Glacier.



Q164. A company is building a transcription service in which a fleet of EC2 worker instances processes an uploaded audio file and generates a text file as an output. They must store both of these frequently accessed files in the same durable storage until the text file is retrieved by the uploader. Due to an expected surge in demand, they have to ensure that the storage is scalable and can be retrieved within minutes.

Which storage option in AWS can they use in this situation, which is both cost-efficient and scalable?

- A. A single Amazon S3 bucket
- B. Amazon S3 Glacier Deep Archive
- C. Multiple Amazon EBS volume with snapshots
- D. Multiple instance stores

Q165. A company plans to conduct a network security audit. The web application is hosted on an Auto Scaling group of EC2 Instances with an Application Load Balancer in front to evenly distribute the incoming traffic. A Solutions Architect has been tasked to enhance the security posture of the company's cloud infrastructure and minimize the impact of DDoS attacks on its resources.

Which of the following is the most effective solution that should be implemented?

A. Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin.

Use VPC Flow Logs to monitor abnormal traffic patterns. Set up a custom AWS Lambda function that processes the flow logs and invokes Amazon SNS for notification.

B. Configure Amazon CloudFront distribution and set a Network Load Balancer as the origin.

Use Amazon GuardDuty to block suspicious hosts based on its security findings. Set up a custom AWS Lambda function that processes the security logs and invokes Amazon SNS for notification.

C. Configure Amazon CloudFront distribution and set an Application Load Balancer as the origin. Create a security group rule and deny all the suspicious addresses. Use Amazon SNS for notification.

D. Configure Amazon CloudFront distribution and set Application Load Balancer as the origin. Create a rate-based web ACL rule using AWS WAF and associate it with Amazon CloudFront.

Q166. A company runs a messaging application in the ap-northeast-1 and ap-southeast-2 region. A Solutions Architect needs to create a routing policy wherein a larger portion of traffic from the Philippines and North India will be routed to the resource in the ap-northeast-1 region. Which Route 53 routing policy should the Solutions Architect use?

- A. Weighted Routing
- B. Geoproximity Routing
- C. Latency Routing
- D. Geolocation Routing

Q167. All objects uploaded to an Amazon S3 bucket must be encrypted for security compliance. The bucket will use server-side encryption with Amazon S3-Managed encryption keys (SSE-S3) to encrypt data using 256-bit Advanced Encryption Standard (AES-256) block cipher.

Which of the following request headers must be used?

- A. x-amz-server-side-encryption-customer-key
- B. x-amz-server-side-encryption
- C. x-amz-server-side-encryption-customer-algorithm
- D. x-amz-server-side-encryption-customer-key-MD5

Q168. A company has a requirement to move 80 TB data warehouse to the cloud. It would take 2 months to transfer the data given their current bandwidth allocation. Which is the most cost-effective service that would allow you to quickly upload their data into AWS?

- A. AWS Snowball Edge
- B. AWS Snowmobile
- C. AWS Direct Connect

## D. Amazon S3 Multipart Upload

Q169. One member of your DevOps team consulted you about a connectivity problem in one of your Amazon EC2 instances. The application architecture is initially set up with four EC2 instances, each with an EIP address that all belong to a public non-default subnet. You launched another instance to handle the increasing workload of your application. The EC2 instances also belong to the same security group. Everything works well as expected except for one of the EC2 instances which is not able to send nor receive traffic over the Internet.

Which of the following is the MOST likely reason for this issue?

- A. The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway.
- B. The EC2 instance does not have a public IP address associated with it.
- C. The EC2 instance does not have a private IP address associated with it.
- D. The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway.

Q170. A start-up company that offers an intuitive financial data analytics service has consulted you about their AWS architecture. They have a fleet of Amazon EC2 worker instances that process financial data and then outputs reports which are used by their clients. You must store the generated report files in a durable storage. The number of files to be stored can grow over time as the

start-up company is expanding rapidly overseas and hence, they also need a way to distribute the reports faster to clients located across the globe.

Which of the following is a cost-efficient and scalable storage option that you should use for this scenario?

- A. Use Amazon S3 as the data storage and CloudFront as the CDN.
- B. Use Amazon Redshift as the data storage and CloudFront as the CDN.
- C. Use Amazon Glacier as the data storage and ElastiCache as the CDN.
- D. Use multiple EC2 instance stores for data storage and ElastiCache as the CDN.

Q171. A company launched a website that accepts high-quality photos and turns them into a downloadable video montage. The website offers a free and a premium account that guarantees faster processing. All requests by both free and premium members go through a single SQS queue and then processed by a group of EC2 instances that generate the videos. The company needs to ensure that the premium users who paid for the service have higher priority than the free members.

How should the company re-design its architecture to address this requirement?

- A. Use Amazon S3 to store and process the photos and then generate the video montage afterward.
- B. Create an SQS queue for free members and another one for premium

members. Configure your EC2 instances to consume messages from the premium queue first and if it is empty, poll from the free members' SQS queue.

C. For the requests made by premium members, set a higher priority in the SQS queue so it will be processed first compared to the requests made by free members.

D. Use Amazon Kinesis to process the photos and generate the video montage in real-time.

Q172. A company has developed public APIs hosted in Amazon EC2 instances behind an Elastic Load Balancer. The APIs will be used by various clients from their respective on-premises data centers. A Solutions Architect received a report that the web service clients can only access trusted IP addresses whitelisted on their firewalls.

What should you do to accomplish the above requirement?

A. Associate an Elastic IP address to an Application Load Balancer.

B. Associate an Elastic IP address to a Network Load Balancer.

C. Create an Alias Record in Route 53 which maps to the DNS name of the load balancer.

D. Create a CloudFront distribution whose origin points to the private IP addresses of your web servers.

Q173. An accounting application uses an RDS database configured with Multi-

AZ deployments to improve availability. What would happen to RDS if the primary database instance fails?

- A. A new database instance is created in the standby Availability Zone.
- B. The canonical name record (CNAME) is switched from the primary to standby instance.
- C. The IP address of the primary DB instance is switched to the standby DB instance.
- D. The primary database instance will reboot.

Q174. A solutions architect is designing a cost-efficient, highly available storage solution for company data. One of the requirements is to ensure that the previous state of a file is preserved and retrievable if a modified version of it is uploaded. Also, to meet regulatory compliance, data over 3 years must be retained in an archive and will only be accessible once a year.

How should the solutions architect build the solution?

- A. Create an S3 Standard bucket with object-level versioning enabled and configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.
- B. Create an S3 Standard bucket and enable S3 Object Lock in governance mode.
- C. Create an S3 Standard bucket with S3 Object Lock in compliance mode enabled then configure a lifecycle rule that transfers files to Amazon S3 Glacier

Deep Archive after 3 years.

D. Create a One-Zone-IA bucket with object-level versioning enabled and configure a lifecycle rule that transfers files to Amazon S3 Glacier Deep Archive after 3 years.

Q175. A company is planning to launch an application which requires a data warehouse that will be used for their infrequently accessed data. You need to use an EBS Volume that can handle large, sequential I/O operations.

Which of the following is the most cost-effective storage type that you should use to meet the requirement?

- A. Cold HDD (sc1)
- B. Throughput Optimized HDD (st1)
- C. Provisioned IOPS SSD (io1)
- D. EBS General Purpose SSD (gp2)

Q176. A company is receiving semi-structured and structured data from different sources every day. The Solutions Architect plans to use big data processing frameworks to analyze vast amounts of data and access it using various business intelligence tools and standard SQL queries. Which of the following provides the MOST high-performing solution that fulfills this requirement?

- A. Use Amazon Kinesis Data Analytics and store the processed data in Amazon



DynamoDB.

B. Use AWS Glue and store the processed data in Amazon S3.

C. Create an Amazon EC2 instance and store the processed data in Amazon EBS.

D. Create an Amazon EMR cluster and store the processed data in Amazon Redshift.

Q177. A company has a dynamic web app written in MEAN stack that is going to be launched in the next month. There is a probability that the traffic will be quite high in the first couple of weeks. In the event of a load failure, how can you set up DNS failover to a static website?

A. Add more servers in case the application fails.

B. Duplicate the exact application architecture in another region and configure DNS weight- based routing.

C. Enable failover to an application hosted in an on-premises data center.

D. Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution.

Q178. A company is running a custom application in an Auto Scaling group of Amazon EC2 instances. Several instances are failing due to insufficient swap space. The Solutions Architect has been instructed to troubleshoot the issue and effectively monitor the available swap space of each EC2 instance.

Which of the following options fulfills this requirement?

- A. Install the CloudWatch agent on each instance and monitor the SwapUtilization metric.
- B. Create a new trail in AWS CloudTrail and configure Amazon CloudWatch Logs to monitor your trail logs.
- C. Create a CloudWatch dashboard and monitor the SwapUsed metric.
- D. Enable detailed monitoring on each instance and monitor the SwapUtilization metric.

Q179. A start-up company has an EC2 instance that is hosting a web application. The volume of users is expected to grow in the coming months and hence, you need to add more elasticity and scalability in your AWS architecture to cope with the demand.

Which of the following options can satisfy the above requirement for the given scenario? (Select TWO.)

- A. Set up an AWS WAF behind your EC2 Instance.
- B. Set up an S3 Cache in front of the EC2 instance.
- C. Set up two EC2 instances deployed using Launch Templates and integrated with AWS Glue.
- D. Set up two EC2 instances and use Route 53 to route traffic based on a Weighted Routing Policy.
- E. Set up two EC2 instances and then put them behind an Elastic Load balancer

(ELB).

Answer DE

Q180. A company recently adopted a hybrid architecture that integrates its on-premises data center to AWS cloud. You are assigned to configure the VPC and implement the required IAM users, IAM roles, IAM groups, and IAM policies.

In this scenario, what is the best practice when creating IAM policies?

- A. Determine what users need to do and then craft policies for them that let the users perform those tasks including additional administrative operations.
- B. Grant all permissions to any EC2 user.
- C. Use the principle of least privilege which means granting only the permissions required to perform a task.
- D. Use the principle of least privilege which means granting only the least number of people with full root access.

Q181. A company has an existing VPC which is quite unutilized for the past few months. The Business Manager instructed the Solutions Architect to integrate the company's on-premises data center and its VPC. The architect explained the list of tasks that he'll be doing and discussed the Virtual Private Network (VPN) connection. The

Business Manager is not tech-savvy but he is interested to know what a VPN

is and its benefits.

What is one of the major advantages of having a VPN in AWS?

- A. It enables you to establish a private and dedicated network connection between your network and your VPC
- B. It provides a cost-effective, hybrid connection from your VPC to your on-premises data centers which bypasses the public Internet.
- C. It allows you to connect your AWS cloud resources to your on-premises data center using secure and private sessions with IP Security (IPSec) or Transport Layer Security (TLS) tunnels.
- D. It provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

Q182. A Solutions Architect is working for a large insurance firm. To maintain compliance with HIPAA laws, all data that is backed up or stored on Amazon S3 needs to be encrypted at rest. In this scenario, what is the best method of encryption for the data, assuming S3 is being used for storing financial-related data? (Select TWO.)

- A. Store the data in encrypted EBS snapshots
- B. Encrypt the data using your own encryption keys then copy the data to Amazon S3 over HTTPS endpoints.
- C. Enable SSE on an S3 bucket to make use of AES-256 encryption
- D. Store the data on EBS volumes with encryption enabled instead of using

## Amazon S3

E. Use AWS Shield to protect your data at rest

Q183. A Solutions Architect working for a startup is designing a High Performance Computing (HPC) application which is publicly accessible for their customers. The startup founders want to mitigate distributed denial- of- service (DDoS) attacks on their application.

Which of the following options are not suitable to be implemented in this scenario? (Select TWO.)

A. Use Dedicated EC2 instances to ensure that each instance has the maximum performance possible.

B. Add multiple Elastic Fabric Adapters (EFA) to each EC2 instance to increase the network bandwidth.

C. Use an Application Load Balancer with Auto Scaling groups for your EC2 instances.

Prevent direct Internet traffic to your Amazon RDS database by deploying it to a new private subnet.

D. Use AWS Shield and AWS WAF.

E. Use an Amazon CloudFront service for distributing both static and dynamic content.

Q184. An application needs to retrieve a subset of data from a large CSV file

stored in an Amazon S3 bucket by using simple SQL expressions. The queries are made within Amazon S3 and must only return the needed data.

Which of the following actions should be taken?

- A. Perform an S3 Select operation based on the bucket's name and object's metadata.
- B. Perform an S3 Select operation based on the bucket's name and object tags.
- C. Perform an S3 Select operation based on the bucket's name.
- D. Perform an S3 Select operation based on the bucket's name and object's key.

Q185. A startup has resources deployed on the AWS Cloud. It is now going through a set of scheduled audits by an external auditing firm for compliance.

Which of the following services available in AWS can be utilized to help ensure the right information are present for auditing purposes?

- A. Amazon CloudWatch
- B. Amazon EC2
- C. Amazon CloudTrail
- D. Amazon VPC

Q186. A large telecommunications company needs to run analytics against all combined log files from the Application Load Balancer as part of the regulatory requirements. Which AWS services can be used together to collect logs and

then easily perform log analysis?

- A. Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application.
- B. Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.
- C. Amazon DynamoDB for storing and EC2 for analyzing the logs.
- D. Amazon EC2 with EBS volumes for storing and analyzing the log files.

Q187. A company deployed a high-performance computing (HPC) cluster that spans multiple EC2 instances across multiple Availability Zones and processes various wind simulation models. Currently, the Solutions Architect is experiencing a slowdown in their applications and upon further investigation, it was discovered that it was due to latency issues.

Which is the MOST suitable solution that the Solutions Architect should implement to provide low-latency network performance necessary for tightly-coupled node-to-node communication of the HPC cluster?

- A. Set up AWS Direct Connect connections across multiple Availability Zones for increased bandwidth throughput and more consistent network experience.
- B. Set up a spread placement group across multiple Availability Zones in multiple AWS Regions.
- C. Set up a cluster placement group within a single Availability Zone in the same AWS Region.

D. Use EC2 Dedicated Instances.

Q188. An investment bank is working with an IT team to handle the launch of the new digital wallet system.

The applications will run on multiple EBS-backed EC2 instances which will store the logs, transactions, and billing statements of the user in an S3 bucket. Due to tight security and compliance requirements, the IT team is exploring options on how to safely store sensitive data on the EBS volumes and S3. Which of the below options should be carried out when storing sensitive data on AWS? (Select TWO.)

- A. Create an EBS Snapshot
- B. Enable Amazon S3 Server-Side or use Client-Side Encryption
- C. Enable EBS Encryption
- D. Migrate the EC2 instances from the public to private subnet.
- E. Use AWS Shield and WAF

Q189. A Solutions Architect is working for a large IT consulting firm. One of the clients is launching a file sharing web application in AWS which requires a durable storage service for hosting their static contents such as PDFs, Word Documents, high-resolution images, and many others. Which type of storage service should the Architect use to meet this requirement?

- A. Amazon RDS instance



- B. Amazon EBS volume
- C. Amazon EC2 instance store
- D. Amazon S3

Q190. An on-premises server is using an SMB network file share to store application data. The application produces around 50 MB of data per day but it only needs to access some of it for daily processes. To save on storage costs, the company plans to copy all the application data to AWS, however, they want to retain the ability to retrieve data with the same low-latency access as the local file share. The company does not have the capacity to develop the needed tool for this operation. Which AWS service should the company use?

- A. AWS Storage Gateway
- B. Amazon FSx for Windows File Server
- C. AWS Virtual Private Network (VPN)
- D. AWS Snowball Edge

Q191. A company is setting up a cloud architecture for an international money transfer service to be deployed in AWS which will have thousands of users around the globe. The service should be available 24/7 to avoid any business disruption and should be resilient enough to handle the outage of an entire AWS region. To meet this requirement, the Solutions Architect has deployed their AWS resources to multiple AWS Regions. He needs to use Route 53 and

configure it to set all of the resources to be available all the time as much as possible. When a resource becomes unavailable, Route 53 should detect that it's unhealthy and stop including it when responding to queries.

Which of the following is the most fault-tolerant routing configuration that the Solutions Architect should use in this scenario?

- A. Configure an Active-Active Failover with One Primary and One Secondary Resource.
- B. Configure an Active-Passive Failover with Multiple Primary and Secondary Resources.
- C. Configure an Active-Passive Failover with Weighted Records.
- D. Configure an Active-Active Failover with Weighted routing policy.

Q192 A company has a global online trading platform in which the users from all over the world regularly

upload terabytes of transactional data to a centralized S3 bucket. What AWS feature should you use in your present system to improve throughput and ensure consistently fast data transfer to the Amazon S3 bucket, regardless of your user's location?

- A. Use CloudFront Origin Access Identity
- B. Amazon S3 Transfer Acceleration
- C. FTP
- D. AWS Direct Connect

Q193. In Amazon EC2, you can manage your instances from the moment you launch them up to their termination. You can flexibly control your computing costs by changing the EC2 instance state. Which of the following statements is true regarding EC2 billing? (Select TWO.)

- A. You will be billed when your Reserved instance is in terminated state.
- B. You will be billed when your Spot instance is preparing to stop with a stopping state.
- C. You will not be billed for any instance usage while an instance is not in the running state.
- D. You will be billed when your On-Demand instance is in pending state.
- E. You will be billed when your On-Demand instance is preparing to hibernate with a stopping state.

Q194. A Solutions Architect for a global news company is configuring a fleet of EC2 instances in a subnet that currently is in a VPC with an Internet gateway attached. All of these EC2 instances can be accessed from the Internet. The architect launches another subnet and deploys an EC2 instance in it, however, the architect

is not able to access the EC2 instance from the Internet.

What could be the possible reasons for this issue? (Select TWO.)

- A. The route table is not configured properly to send traffic from the EC2

instance to the Internet through the Internet gateway.

B. The Amazon EC2 instance does not have a public IP address associated with it.

C. The Amazon EC2 instance is not a member of the same Auto Scaling group.

D. The Amazon EC2 instance does not have an attached Elastic Fabric Adapter (EFA).

E. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the customer gateway (CGW).

Q195. A company has clients all across the globe that access product files stored in several S3 buckets, which are behind each of their own CloudFront web distributions. They currently want to deliver their content to a specific client, and they need to make sure that only that client can access the data. Currently, all of their clients can access their S3 buckets directly using an S3 URL or through their CloudFront distribution. The Solutions Architect must serve the private content via CloudFront only, to secure the distribution of files. Which combination of actions should the Architect implement to meet the above requirements? (Select TWO.)

A. Use S3 pre-signed URLs to ensure that only their client can access the files. Remove permission to use Amazon S3 URLs to read the files for anyone else.

B. Use AWS App Mesh to ensure that only their client can access the files.

C. Restrict access to files in the origin by creating an origin access identity (OAI)

and give it permission to read the files in the bucket.

D. Use AWS Cloud Map to ensure that only their client can access the files.

E. Require the users to access the private content by using special CloudFront signed URLs or signed cookies.

Q196. A company plans to use a durable storage service to store on-premises database backups to the AWS cloud.

To move their backup data, they need to use a service that can store and retrieve objects through standard file storage protocols for quick recovery.

Which of the following options will meet this requirement?

A. Use Amazon EBS volumes to store all the backup data and attach it to an Amazon EC2 instance.

B. Use AWS Snowball Edge to directly backup the data in Amazon S3 Glacier.

C. Use the AWS Storage Gateway file gateway to store all the backup data in Amazon S3.

D. Use the AWS Storage Gateway volume gateway to store the backup data and directly access it using Amazon S3 API actions.

Q197. A large insurance company has an AWS account that contains three VPCs (DEV, UAT and PROD) in the same region. UAT is peered to both PROD and DEV using a VPC peering connection. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to

Prod to speed up time to market. Which of the following options helps the company accomplish this?

- A. Change the DEV and PROD VPCs to have overlapping CIDR blocks to be able to connect them.
- B. Create a new VPC peering connection between PROD and DEV with the appropriate routes.
- C. Create a new entry to PROD in the DEV route table using the VPC peering connection as the target.
- D. Do nothing. Since these two VPCs are already connected via UAT, they already have a connection to each other.

Q198. Due to the large volume of query requests, the database performance of an online reporting application significantly slowed down. The Solutions Architect is trying to convince her client to use Amazon RDS Read Replica for their application instead of setting up a Multi-AZ Deployments configuration. What are two benefits of using Read Replicas over Multi-AZ that the Architect should point out? (Select TWO.)

- A. It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator.
- B. Allows both read and write operations on the read replica to complement the primary database.
- C. Provides synchronous replication and automatic failover in the case of

Availability Zone service failures.

D. Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.

E. It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

Q199. A major TV network has a web application running on eight Amazon T3 EC2 instances. The number of requests that the application processes are consistent and do not experience spikes. To ensure that eight instances are running at all times, the Solutions Architect should create an Auto Scaling group and distribute the load evenly between all instances.

Which of the following options can satisfy the given requirements?

A. Deploy eight EC2 instances with Auto Scaling in one Availability Zone behind an Amazon Elastic Load Balancer.

B. Deploy four EC2 instances with Auto Scaling in one region and four in another region behind an Amazon Elastic Load Balancer.

C. Deploy two EC2 instances with Auto Scaling in four regions behind an Amazon Elastic Load Balancer.

D. Deploy four EC2 instances with Auto Scaling in one Availability Zone and four in another availability zone in the same region behind an Amazon Elastic Load Balancer.

Q200. An aerospace engineering company recently adopted a hybrid cloud infrastructure with AWS. One of the Solutions Architect's tasks is to launch a VPC with both public and private subnets for their EC2 instances as well as their database instances.

Which of the following statements are true regarding Amazon VPC subnets?

(Select TWO.)

- A. Each subnet spans to 2 Availability Zones.
- B. EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP.
- C. The allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /27 netmask (32 IP addresses).
- D. Each subnet maps to a single Availability Zone.
- E. Every subnet that you create is automatically associated with the main route table for the VPC.

Q201. A company plans to set up a cloud infrastructure in AWS. In the planning, it was discussed that you need to deploy two EC2 instances that should continuously run for three years. The CPU utilization of the EC2 instances is also expected to be stable and predictable.

Which is the most cost-efficient Amazon EC2 Pricing type that is most appropriate for this scenario?

- A. Spot instances



- B. Reserved Instances
- C. Dedicated Hosts
- D. On-Demand instances

Q202. A Solutions Architect is unable to connect to the newly deployed EC2 instance via SSH using a home computer. However, the Architect was able to successfully access other existing instances in the VPC without any issues.

Which of the following should the Architect check and possibly correct to restore connectivity?

- A. Configure the Security Group of the EC2 instance to permit ingress traffic over port 22 from your IP.
- B. Configure the Network Access Control List of your VPC to permit ingress traffic over port 22 from your IP.
- C. Use Amazon Data Lifecycle Manager.
- D. Configure the Security Group of the EC2 instance to permit ingress traffic over port 3389 from your IP.

Q203. A Solutions Architect needs to deploy a mobile application that can collect votes for a popular singing competition. Millions of users from around the world will submit votes using their mobile phones. These votes must be collected and stored in a highly scalable and highly available data store which will be queried for realtime ranking.

Which of the following combination of services should the architect use to meet this requirement?

- A. Amazon Redshift and AWS Mobile Hub
- B. Amazon Relational Database Service (RDS) and Amazon MQ
- C. Amazon Aurora and Amazon Cognito
- D. Amazon DynamoDB and AWS AppSync

Q204. A FinTech startup deployed an application on an Amazon EC2 instance with attached Instance Store volumes and an Elastic IP address. The server is only accessed from 8 AM to 6 PM and can be stopped from 6 PM to 8 AM for cost efficiency using Lambda with the script that automates this based on tags. Which of the following will occur when the EC2 instance is stopped and started? (Select TWO.)

- A. The underlying host for the instance is possibly changed.
- B. The ENI (Elastic Network Interface) is detached.
- C. All data on the attached instance-store devices will be lost.
- D. The Elastic IP address is disassociated with the instance.
- E. There will be no changes.

Q205. A media company recently launched their newly created web application. Many users tried to visit the website, but they are receiving a 503 Service Unavailable Error. The system administrator tracked the EC2 instance status

and saw the capacity is reaching its maximum limit and unable to process all the requests. To gain insights from the application's data, they need to launch a real-time analytics service. Which of the following allows you to read records in batches?

- A. Create a Kinesis Data Stream and use AWS Lambda to read records from the data stream.
- B. Create an Amazon S3 bucket to store the captured data and use Amazon Athena to analyze the data.
- C. Create a Kinesis Data Firehose and use AWS Lambda to read records from the data stream.
- D. Create an Amazon S3 bucket to store the captured data and use Amazon Redshift Spectrum to analyze the data.

Q206. The media company that you are working for has a video transcoding application running on Amazon EC2. Each EC2 instance polls a queue to find out which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video will be transcoded by another instance based on the queuing system. This application has a large backlog of videos which need to be transcoded. Your manager would like to reduce this backlog by adding more EC2 instances, however, these instances are only needed until the backlog is reduced.

In this scenario, which type of Amazon EC2 instance is the most cost-effective type to use?

- A. Spot instances
- B. Reserved instances
- C. Dedicated instances
- D. On-demand instances

Q207. A company has an On-Demand EC2 instance located in a subnet in AWS that hosts a web application. The security group attached to this EC2 instance has the following Inbound Rules:

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	

The Route table attached to the VPC is shown below. You can establish an SSH connection into the EC2 instance from the Internet. However, you are not able to connect to the web server using your Chrome browser.

Destination	Target	Status	Propagated
10.0.0.0/27	local	Active	No
0.0.0.0/0	lgw-b51618cc	Active	No

Which of the below steps would resolve the issue?

- A. In the Route table, add this new route entry: 10.0.0.0/27 -> local

B. In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc

C. In the Security Group, add an Inbound HTTP rule.

D. In the Security Group, remove the SSH rule.

Q208. A company is hosting EC2 instances that are on non-production environment and processing non-priority batch loads, which can be interrupted at any time.

What is the best instance purchasing option which can be applied to your EC2 instances in this case?

A. Spot Instances

B. On-Demand Capacity Reservations

C. Reserved Instances

D. On-Demand Instances

Q209. A manufacturing company has EC2 instances running in AWS. The EC2 instances are configured with Auto Scaling. There are a lot of requests being lost because of too much load on the servers. The Auto Scaling is launching new EC2 instances to take the load accordingly yet, there are still some requests that are being lost.

Which of the following is the MOST suitable solution that you should implement to avoid losing recently submitted requests?

A. Set up Amazon Aurora Serverless for on-demand, auto-scaling configuration

of your EC2 Instances and also enable Amazon Aurora Parallel Query feature for faster analytical queries over your current data.

B. Use an Amazon SQS queue to decouple the application components and scale-out the EC2 instances based upon the ApproximateNumberOfMessages metric in Amazon CloudWatch.

C. Use larger instances for your application with an attached Elastic Fabric Adapter (EFA).

D. Replace the Auto Scaling group with a cluster placement group to achieve a low-latency network performance necessary for tightly-coupled node-to-node communication.

Q210. A travel company has a suite of web applications hosted in an Auto Scaling group of On-Demand EC2

instances behind an Application Load Balancer that handles traffic from various web domains such as i-lovemanila.com, i-love-boracay.com, i-love-cebu.com and many others. To improve security and lessen the overall cost, you are instructed to secure the system by allowing multiple domains to serve SSL traffic without the need to reauthenticate and reprovision your certificate everytime you add a new domain. This migration from HTTP to HTTPS will help improve their SEO and Google search ranking. Which of the following is the most costeffective solution to meet the above requirement?

A. Use a wildcard certificate to handle multiple sub-domains and different

domains.

B. Add a Subject Alternative Name (SAN) for each additional domain to your certificate.

C. Upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).

D. Create a new CloudFront web distribution and configure it to serve HTTPS requests using dedicated IP addresses in order to associate your alternate domain names with a dedicated IP address in each CloudFront edge location.

Q211. A new online banking platform has been re-designed to have a microservices architecture in which complex applications are decomposed into smaller, independent services. The new platform is using Docker considering that application containers are optimal for running small, decoupled services. The new solution should remove the need to provision and manage servers, let you specify and pay for resources per application, and improve security through application isolation by design. Which of the following is the MOST suitable service to use to migrate this new platform to AWS?

A. Amazon EBS

B. Amazon EFS

C. Amazon EKS

## D. AWS Fargate

Q212. A company has established a dedicated network connection from its on-premises data center to AWS Cloud

using AWS Direct Connect (DX). The core network services, such as the Domain Name System (DNS) service and Active Directory services, are all hosted on-premises. The company has new AWS accounts that will also require consistent and dedicated access to these network services. Which of the following can satisfy this requirement with the LEAST amount of operational overhead and in a cost-effective manner?

A. Create a new AWS VPN CloudHub. Set up a Virtual Private Network (VPN) connection for additional AWS accounts.

B. Set up a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Configure a VPC peering connection between AWS accounts and associate it with Direct Connect gateway.

C. Set up another Direct Connect connection for each and every new AWS account that will be added.

D. Create a new Direct Connect gateway and integrate it with the existing Direct Connect connection. Set up a Transit Gateway between AWS accounts and associate it with the Direct Connect gateway.

213. A company is storing its financial reports and regulatory documents in an



Amazon S3 bucket. To comply with the IT audit, they tasked their Solutions Architect to track all new objects added to the bucket as well as the removed ones. It should also track whether a versioned object is permanently deleted. The Architect must configure Amazon S3 to publish notifications for these events to a queue for post-processing and to an Amazon SNS topic that will notify the Operations team.

Which of the following is the MOST suitable solution that the Architect should implement?

- A. Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS.
- B. Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS.
- C. Create a new Amazon SNS topic and Amazon MQ. Add an S3 event notification configuration on the bucket to publish s3:ObjectAdded:\* and s3:ObjectRemoved:\* event types to SQS and SNS.
- D. Create a new Amazon SNS topic and Amazon SQS queue. Add an S3 event notification configuration on the bucket to publish s3:ObjectCreated:\* and s3:ObjectRemoved:Delete event types to SQS and SNS.

Q214. A data analytics company is setting up an innovative checkout-free

grocery store. Their Solutions Architect developed a real-time monitoring application that uses smart sensors to collect the items that the customers are getting from the grocery's refrigerators and shelves then automatically deduct it from their accounts. The company wants to analyze the items that are frequently being bought and store the results in S3 for durable storage to determine the purchase behavior of its customers. What service must be used to easily capture, transform, and load streaming data into Amazon S3, Amazon Elasticsearch Service, and Splunk?

- A. Amazon Kinesis Data Firehose
- B. Amazon Redshift
- C. Amazon Kinesis
- D. Amazon SQS

Q215. A company is using Amazon VPC that has a CIDR block of 31.0.0/27 that is connected to the on-premises data center. There was a requirement to create a Lambda function that will process massive amounts of cryptocurrency transactions every minute and then store the results to EFS. After setting up the serverless architecture and connecting the Lambda function to the VPC, the Solutions Architect noticed an increase in invocation errors with EC2 error types such as `EC2ThrottledException` at certain times of the day.

Which of the following are the possible causes of this issue? (Select TWO.)

- A. You only specified one subnet in your Lambda function configuration. That

single subnet runs out of available IP addresses and there is no other subnet or Availability Zone which can handle the peak load.

B. The attached IAM execution role of your function does not have the necessary permissions to access the resources of your VPC.

C. The associated security group of your function does not allow outbound connections.

D. Your VPC does not have sufficient subnet ENIs or subnet IPs.

E. E. Your VPC does not have a NAT gateway.

Q216. A tech startup is launching an on-demand food delivery platform using Amazon ECS cluster with an AWS Fargate serverless compute engine and Amazon Aurora. It is expected that the database read queries will significantly increase in the coming weeks ahead. A Solutions Architect recently launched two Read Replicas to the database cluster to improve the platform's scalability. Which of the following is the MOST suitable configuration that the Architect should implement to load balance all of the incoming read requests equally to the two Read Replicas?

A. Use the built-in Reader endpoint of the Amazon Aurora database.

B. Enable Amazon Aurora Parallel Query.

C. Create a new Network Load Balancer to evenly distribute the read queries to the Read Replicas of the Amazon Aurora database.

D. Use the built-in Cluster endpoint of the Amazon Aurora database.

Q217. A company is using multiple AWS accounts that are consolidated using AWS Organizations. They want to copy several S3 objects to another S3 bucket that belonged to a different AWS account which they also own. The Solutions Architect was instructed to set up the necessary permissions for this task and to ensure that the destination account owns the copied objects and not the account it was sent from. How can the Architect accomplish this requirement?

A. Set up cross-origin resource sharing (CORS) in S3 by creating a bucket policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account.

B. Enable the Requester Pays feature in the source S3 bucket. The fees would be waived through Consolidated Billing since both AWS accounts are part of AWS Organizations.

C. Configure cross-account permissions in S3 by creating an IAM customer-managed policy that allows an IAM user or role to copy objects from the source bucket in one account to the destination bucket in the other account. Then attach the policy to the IAM user or role that you want to use to copy objects between accounts.

D. Connect the two S3 buckets from two different AWS accounts to Amazon WorkDocs. Set up cross- account access to integrate the two S3 buckets. Use the Amazon WorkDocs console to copy the objects from one account to the other with modified object ownership assigned to the destination account.

Q218. A document sharing website is using AWS as its cloud infrastructure. Free users can upload a total of 5 GB data while premium users can upload as much as 5 TB. Their application uploads the user files, which can have a max file size of 1 TB, to an S3 Bucket.

In this scenario, what is the best way for the application to upload the large files in S3?

- A. Use Multipart Upload
- B. Use a single PUT request to upload the large file
- C. Use AWS Import/Export
- D. Use AWS Snowball

Q219. A solutions architect is formulating a strategy for a startup that needs to transfer 50 TB of on-premises data to Amazon S3. The startup has a slow network transfer speed between its data center and AWS which causes a bottleneck for data migration.

Which of the following should the solutions architect implement?

- A. Integrate AWS Storage Gateway File Gateway with the on-premises data center.
- B. Request an Import Job to Amazon S3 using a Snowball device in the AWS Snowball Console.
- C. Enable Amazon S3 Transfer Acceleration on the target S3 bucket.

D. Deploy an AWS Migration Hub Discovery agent in the on-premises data center.

Q220. A global online sports betting company has its popular web application hosted in AWS. They are planning to develop a new online portal for their new business venture and they hired you to implement the cloud architecture for a new online portal that will accept bets globally for world sports. You started to design the system with a relational database that runs on a single EC2 instance, which requires a single EBS volume that can support up to 30,000 IOPS.

In this scenario, which Amazon EBS volume type can you use that will meet the performance requirements of this new online portal?

- A. EBS General Purpose SSD (gp2)
- B. EBS Cold HDD (sc1)
- C. EBS Provisioned IOPS SSD (io1)
- D. EBS Throughput Optimized HDD (st1)

Q221. A company needs to use Amazon Aurora as the Amazon RDS database engine of their web application.

The Solutions Architect has been instructed to implement a 90-day backup retention policy. Which of the following options can satisfy the given requirement?

- A. Configure an automated backup and set the backup retention period to 90

days.

B. Create a daily scheduled event using CloudWatch Events and AWS Lambda to directly download the RDS automated snapshot to an S3 bucket. Archive snapshots older than 90 days to Glacier.

C. Configure RDS to export the automated snapshot automatically to Amazon S3 and create a lifecycle policy to delete the object after 90 days.

D. Create an AWS Backup plan to take daily snapshots with a retention period of 90 days.

Q222. A company is deploying a Microsoft SharePoint Server environment on AWS using CloudFormation. The Solutions Architect needs to install and configure the architecture that is composed of Microsoft Active Directory (AD) domain controllers, Microsoft SQL Server 2012, multiple Amazon EC2 instances to host the Microsoft SharePoint Server and many other dependencies. The Architect needs to ensure that the required components are properly running before the stack creation proceeds. Which of the following should the Architect do to meet this requirement?

A. Configure the UpdateReplacePolicy attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.

B. Configure the DependsOn attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-

init helper script.

C. Configure a CreationPolicy attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.

D. Configure a UpdatePolicy attribute to the instance in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-signal helper script.

Q223. A company needs to collect gigabytes of data per second from websites and social media feeds to gain insights on its product offerings and continuously improve the user experience. To meet this design requirement, you have developed an application hosted on an Auto Scaling group of Spot EC2 instances which processes the data and stores the results to DynamoDB and Redshift. The solution should have a built-in enhanced fan-out feature.

Which fully-managed AWS service can you use to collect and process large streams of data records in real- time with the LEAST amount of administrative overhead?

- A. Amazon Redshift with AWS Cloud Development Kit (AWS CDK)
- B. Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- C. Amazon Kinesis Data Streams
- D. Amazon S3 Access Points



Q224. A company plans to build a web architecture using On-Demand EC2 instances and a database in AWS. However, due to budget constraints, the company instructed the Solutions Architect to choose a database service in which they no longer need to worry about database management tasks such as hardware or software provisioning, setup, configuration, scaling, and backups. Which of the following services should the Solutions Architect recommend?

- A. Amazon ElastiCache
- B. Amazon DynamoDB
- C. Amazon RDS
- D. Amazon Redshift

Q225. A tech company is currently using Auto Scaling for their web application. A new AMI now needs to be used for launching a fleet of EC2 instances. Which of the following changes needs to be done?

- A. Create a new target group.
- B. Do nothing. You can start directly launching EC2 instances in the Auto Scaling group with the same launch configuration.
- C. Create a new launch configuration.
- D. Create a new target group and launch configuration.

Q226. A large financial firm needs to set up a Linux bastion host to allow access

to the Amazon EC2 instances running in their VPC. For security purposes, only the clients connecting from the corporate external public IP address 175.45.116.100 should have SSH access to the host. Which is the best option that can meet the customer's requirement?

- A. Security Group Inbound Rule: Protocol ?UDP, Port Range ?22, Source45.116.100/32
- B. Security Group Inbound Rule: Protocol ?TCP. Port Range ?22, Source45.116.100/32
- C. Network ACL Inbound Rule: Protocol ?TCP, Port Range-22, Source45.116.100/0
- D. Network ACL Inbound Rule: Protocol ?UDP, Port Range ?22, Source45.116.100/32

Q227. A Solutions Architect is managing a company's AWS account of approximately 300 IAM users. They have a new company policy that requires changing the associated permissions of all 100 IAM users that control the access to Amazon S3 buckets.

What will the Solutions Architect do to avoid the time-consuming task of applying the policy to each user?

- A. Create a new policy and apply it to multiple IAM users using a shell script.
- B. Create a new S3 bucket access policy with unlimited access for each IAM user.

- C. Create a new IAM role and add each user to the IAM role.
- D. Create a new IAM group and then add the users that require access to the S3 bucket.

Afterward, apply the policy to the IAM group.

Q228. A company needs to launch an Amazon EC2 instance with persistent block storage to host its application.

The stored data must be encrypted at rest.

Which of the following is the most suitable storage solution in this scenario?

- A. Amazon EBS volume with server-side encryption (SSE) enabled.
- B. Amazon EC2 Instance Store with SSL encryption.
- C. Encrypted Amazon EBS volume using AWS KMS.
- D. Encrypted Amazon EC2 Instance Store using AWS KMS.

Q229. A company is generating confidential data that is saved on their on-premises data center. As a backup solution, the company wants to upload their data to an Amazon S3 bucket. In compliance with its internal security mandate, the encryption of the data must be done before sending it to Amazon S3. The company must spend time managing and rotating the encryption keys as well as controlling who can access those keys.

Which of the following methods can achieve this requirement? (Select TWO.)

- A. Set up Client-Side Encryption using a client-side master key.

- B. Set up Client-Side Encryption with a customer master key stored in AWS Key Management Service (AWS KMS).
- C. Set up Client-Side Encryption with Amazon S3 managed encryption keys.
- D. Set up Server-Side Encryption (SSE) with EC2 key pair.
- E. Set up Server-Side Encryption with keys stored in a separate S3 bucket.

Q230. A company deployed several EC2 instances in a private subnet. The Solutions Architect needs to ensure the

100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	Custom TCP Rule	TCP (6)	4000	110.238.109.37/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

security

of all EC2 instances. Upon checking the existing Inbound Rules of the Network ACL, she saw this configuration:

If a computer with an IP address of 110.238.109.37 sends a request to the VPC, what will happen?

- A. Initially, it will be allowed and then after a while, the connection will be denied.
- B. It will be denied.
- C. Initially, it will be denied and then after a while, the connection will be allowed.
- D. It will be allowed.

Q231. A company currently has an Augment Reality (AR) mobile game that has

a serverless backend. It is using a DynamoDB table which was launched using the AWS CLI to store all the user data and information gathered from the players and a Lambda function to pull the data from DynamoDB. The game is being used by millions of users each day to read and store data.

How would you design the application to improve its overall performance and make it more scalable while keeping the costs low? (Select TWO.)

- A. Enable DynamoDB Accelerator (DAX) and ensure that the Auto Scaling is enabled and increase the maximum provisioned read and write capacity.
- B. Configure CloudFront with DynamoDB as the origin; cache frequently accessed data on the client device using ElastiCache.
- C. Use API Gateway in conjunction with Lambda and turn on the caching on frequently accessed data and enable DynamoDB global replication.
- D. Use AWS SSO and Cognito to authenticate users and have them directly access DynamoDB using single-sign on. Manually set the provisioned read and write capacity to a higher RCU and WCU.
- E. Since Auto Scaling is enabled by default, the provisioned read and write capacity will adjust automatically. Also enable DynamoDB Accelerator (DAX) to improve the performance from milliseconds to microseconds.

Q232. A large financial firm in the country has an AWS environment that contains several Reserved EC2 instances hosting a web application that has been decommissioned last week. To save costs, you need to stop incurring

charges for the Reserved instances as soon as possible. What cost-effective steps will you take in this circumstance? (Select TWO.)

- A. Contact AWS to cancel your AWS subscription.
- B. Go to the Amazon.com online shopping website and sell the Reserved instances.
- C. Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.
- D. Terminate the Reserved instances as soon as possible to avoid getting billed at the on- demand price when it expires.
- E. Stop the Reserved instances as soon as possible.

Q233. A Solutions Architect needs to set up a bastion host in the cheapest, most secure way. The Architect should be the only person that can access it via SSH.

Which of the following steps would satisfy this requirement?

- A. Set up a large EC2 instance and a security group that only allows access on port 22
- B. Set up a large EC2 instance and a security group that only allows access on port 22 via your IP address
- C. Set up a small EC2 instance and a security group that only allows access on port 22 via your IP address
- D. Set up a small EC2 instance and a security group that only allows access on

port 22

Q234. An online stocks trading application that stores financial data in an S3 bucket has a lifecycle policy that moves older data to Glacier every month. There is a strict compliance requirement where a surprise audit can happen at anytime and you should be able to retrieve the required data in under 15 minutes under all circumstances. Your manager instructed you to ensure that retrieval capacity is available when you need it and should handle up to 150 MB/s of retrieval throughput.

Which of the following should you do to meet the above requirement? (Select TWO.)

- A. Specify a range, or portion, of the financial data archive to retrieve.
- B. Use Bulk Retrieval to access the financial data.
- C. Purchase provisioned retrieval capacity.
- D. Retrieve the data using Amazon Glacier Select.
- E. Use Expedited Retrieval to access the financial data.

Q235. A company has a web application that is relying entirely on slower disk-based databases, causing it to perform slowly. To improve its performance, the Solutions Architect integrated an in-memory data store to the web application using ElastiCache.

How does Amazon ElastiCache improve database performance?

- A. By caching database query results.

B. It reduces the load on your database by routing read queries from your applications to the Read Replica.

C. It securely delivers data to customers globally with low latency and high transfer speeds.

D. It provides an in-memory cache that delivers up to 10x performance improvement from milliseconds to microseconds or even at millions of requests per second.

Q236. You are automating the creation of EC2 instances in your VPC. Hence, you wrote a python script to trigger the Amazon EC2 API to request 50 EC2 instances in a single Availability Zone. However, you noticed that after 20 successful requests, subsequent requests failed. What could be a reason for this issue and how would you resolve it?

A. By default, AWS allows you to provision a maximum of 20 instances per region. Select a different region and retry the failed request.

B. There was an issue with the Amazon EC2 API. Just resend the requests and these will be provisioned successfully.

C. By default, AWS allows you to provision a maximum of 20 instances per Availability Zone. Select a different Availability Zone and retry the failed request.

D. There is a vCPU-based On-Demand Instance limit per region which is why subsequent requests failed.

Just submit the limit increase form to AWS and retry the failed requests once



approved.

Q237. A company has a decoupled application in AWS using EC2, Auto Scaling group, S3, and SQS. The Solutions Architect designed the architecture in such a way that the EC2 instances will consume the message from the SQS queue and will automatically scale up or down based on the number of messages in the queue.

In this scenario, which of the following statements is false about SQS?

- A. Amazon SQS can help you build a distributed application with decoupled components.
- B. FIFO queues provide exactly-once processing.
- C. Standard queues preserve the order of messages.
- D. Standard queues provide at-least-once delivery, which means that each message is delivered at least once.

Q238. A production MySQL database hosted on Amazon RDS is running out of disk storage. The management has consulted its solutions architect to increase the disk space without impacting the database performance.

How can the solutions architect satisfy the requirement with the LEAST operational overhead?

- A. Change the default\_storage\_engine of the DB instance's parameter group to MyISAM.

- B. Modify the DB instance storage type to Provisioned IOPS.
- C. Modify the DB instance settings and enable storage autoscaling.
- D. Increase the allocated storage for the DB instance.

Q239. A company installed sensors to track the number of people who visit the park. The data is sent every day to an Amazon Kinesis stream with default settings for processing, in which a consumer is configured to process the data every other day. You noticed that the S3 bucket is not receiving all of the data that is being sent to the Kinesis stream. You checked the sensors if they are properly sending the data to Amazon Kinesis and verified that the data is indeed sent every day. What could be the reason for this?

- A. By default, Amazon S3 stores the data for 1 day and moves it to Amazon Glacier.
- B. There is a problem in the sensors. They probably had some intermittent connection hence, the data is not sent to the stream.
- C. By default, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream.
- D. Your AWS account was hacked and someone has deleted some data in your Kinesis stream.

Q240. An auto scaling group of Linux EC2 instances is created with basic monitoring enabled in CloudWatch. You noticed that your application is slow so

you asked one of your engineers to check all of your EC2 instances. After checking your instances, you noticed that the auto scaling group is not launching more instances as it should be, even though the servers already have high memory usage. Which of the following options should the Architect implement to solve this issue?

- A. Enable detailed monitoring on the instances.
- B. Install AWS SDK in the EC2 instances. Create a script that will trigger the Auto Scaling event if there is high memory usage.
- C. Modify the scaling policy to increase the threshold to scale out the number of instances.
- D. Install the CloudWatch agent to the EC2 instances which will trigger your Auto Scaling group to scale out.

Q241. A technical lead of the Cloud Infrastructure team was consulted by a software developer regarding the required AWS resources of the web application that he is building. The developer knows that an Instance Store only provides ephemeral storage where the data is automatically deleted when the instance is terminated. To ensure that the data of the web application persists, the app should be launched in an EC2 instance that has a durable, block-level storage volume attached. The developer knows that they need to use an EBS volume, but they are not sure what type they need to use. In this scenario, which of the following is true about Amazon EBS volume types and

their respective usage? (Select TWO.)

A. Single root I/O virtualization (SR-IOV) volumes are suitable for a broad range of workloads, including small to medium-sized databases, development and test environments, and boot volumes.

B. Provisioned IOPS volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases.

C. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.

D. General Purpose SSD (gp3) volumes with multi-attach enabled offer consistent and low-latency performance, and are designed for applications requiring multi-az resiliency.

E. Spot volumes provide the lowest cost per gigabyte of all EBS volume types and are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.

Q242. A Fortune 500 company which has numerous offices and customers around the globe has hired you as their Principal Architect. You have staff and customers that upload gigabytes to terabytes of data to a centralized S3 bucket from the regional data centers, across continents, all over the world on a regular basis. At the end of the financial year, there are thousands of data being

uploaded to the central S3 bucket which is in apsoutheast-2 (Sydney) region and a lot of employees are starting to complain about the slow upload times. You were instructed by the CTO to resolve this issue as soon as possible to avoid any delays in processing their global end of financial year (EOFY) reports. Which feature in Amazon S3 enables fast, easy, and secure transfer of your files over long distances between your client and your Amazon S3 bucket?

- A. Cross-Region Replication
- B. Multipart Upload
- C. AWS Global Accelerator
- D. Transfer Acceleration

Q243. A company has a web-based order processing system that is currently using a standard queue in Amazon SQS. The IT Manager noticed that there are a lot of cases where an order was processed twice. This issue has caused a lot of trouble in processing and made the customers very unhappy. The manager has asked you to ensure that this issue will not recur.

What can you do to prevent this from happening again in the future? (Select TWO.)

- A. Alter the visibility timeout of SQS.
- B. Alter the retention period in Amazon SQS.

- C. Replace Amazon SQS and instead, use Amazon Simple Workflow service.
- D. Use an Amazon SQS FIFO Queue instead.
- E. Change the message size in SQS.

Q244. An online trading platform with thousands of clients across the globe is hosted in AWS. To reduce latency, you have to direct user traffic to the nearest application endpoint to the client. The traffic should be routed to the closest edge location via an Anycast static IP address. AWS Shield should also be integrated into the solution for DDoS protection.

Which of the following is the MOST suitable service that the Solutions Architect should use to satisfy the above requirements?

- A. AWS WAF
- B. Amazon CloudFront
- C. AWS PrivateLink
- D. AWS Global Accelerator

Q245. A company launched an online platform that allows people to easily buy, sell, spend, and manage their cryptocurrency. To meet the strict IT audit requirements, each of the API calls on all of the AWS resources should be properly captured and recorded. You used CloudTrail in the VPC to help you in the compliance, operational auditing, and risk auditing of your AWS account. In this scenario, where does CloudTrail store all of the logs that it creates?

- A. DynamoDB

- B. Amazon S3
- C. Amazon Redshift
- D. A RDS instance

Q246. An application is using a RESTful API hosted in AWS which uses Amazon API Gateway and AWS Lambda. There is a requirement to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services.

Which of the following is the most suitable service to use to meet this requirement?

- A. CloudWatch
- B. CloudTrail
- C. AWS X-Ray
- D. VPC Flow Logs

Q247. A real-time data analytics application is using AWS Lambda to process data and store results in JSON format to an S3 bucket. To speed up the existing workflow, you have to use a service where you can run sophisticated Big Data analytics on your data without moving them into a separate analytics system.

Which of the following group of services can you use to meet this requirement?

- A. Amazon X-Ray, Amazon Neptune, DynamoDB
- B. S3 Select, Amazon Neptune, DynamoDB DAX

C. Amazon Glue, Glacier Select, Amazon Redshift

D. S3 Select, Amazon Athena, Amazon Redshift Spectrum

Q248. A company has a High Performance Computing (HPC) cluster that is composed of EC2 Instances with Provisioned IOPS volume to process transaction-intensive, low-latency workloads. The Solutions Architect must maintain high IOPS while keeping the latency down by setting the optimal queue length for the volume. The size of each volume is 10 GiB.

Which of the following is the MOST suitable configuration that the Architect should set up?

A. Set the IOPS to 400 then maintain a low queue length.

B. Set the IOPS to 500 then maintain a low queue length.

C. Set the IOPS to 800 then maintain a low queue length.

D. Set the IOPS to 600 then maintain a high queue length.

Q249. A Solutions Architect is designing the cloud architecture for the enterprise application suite of the company. Both the web and application tiers need to access the Internet to fetch data from public APIs. However, these servers should be inaccessible from the Internet.

Which of the following steps should the Architect implement to meet the above requirements?

A. Deploy the web and application tier instances to a public subnet and then



allocate an Elastic IP address to each EC2 instance.

B. Deploy the web and application tier instances to a private subnet and then allocate an Elastic IP address to each EC2 instance.

C. Deploy a NAT gateway in the private subnet and add a route to it from the public subnet where the web and application tiers are hosted.

D. Deploy a NAT gateway in the public subnet and add a route to it from the private subnet where the web and application tiers are hosted.

Q250. A company has a web application hosted in AWS cloud where the application logs are sent to Amazon CloudWatch. Lately, the web application has recently been encountering some errors which can be resolved simply by restarting the instance.

What will you do to automatically restart the EC2 instances whenever the same application error occurs?

A. First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which invokes an action to restart the EC2 instance.

B. First, look at the existing CloudWatch logs for keywords related to the application error to create a custom metric. Then, create an alarm in Amazon SNS for that custom metric which invokes an action to restart the EC2 instance.

C. First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that

custom metric which invokes an action to restart the EC2 instance.

D. First, look at the existing Flow logs for keywords related to the application error to create a custom metric. Then, create a CloudWatch alarm for that custom metric which calls a Lambda function that invokes an action to restart the EC2 instance.

Q251. A company has hundreds of VPCs with multiple VPN connections to their data centers spanning 5 AWS Regions. As the number of its workloads grows, the company must be able to scale its networks across multiple accounts and VPCs to keep up. A Solutions Architect is tasked to interconnect all of the company's on-premises networks, VPNs, and VPCs into a single gateway, which includes support for inter- region peering across multiple AWS regions. Which of the following is the BEST solution that the architect should set up to support the required interconnectivity?

A. Set up an AWS VPN CloudHub for inter-region VPC access and a Direct Connect gateway for the VPN connections to the on-premises data centers. Create a virtual private gateway in each VPC, then create a private virtual interface for each AWS Direct Connect connection to the Direct Connect gateway.

B. Set up an AWS Direct Connect Gateway to achieve inter-region VPC access to all of the AWS resources and onpremises data centers. Set up a link aggregation group (LAG) to aggregate multiple connections at a single AWS

Direct Connect endpoint in order to treat them as a single, managed connection. Launch a virtual private gateway in each VPC and then create a public virtual interface for each AWS Direct Connect connection to the Direct Connect Gateway.

C. Enable inter-region VPC peering that allows peering relationships to be established between multiple VPCs across different AWS regions. Set up a networking configuration that ensures that the traffic will always stay on the global AWS backbone and never traverse the public Internet.

D. Set up an AWS Transit Gateway in each region to interconnect all networks within it. Then, route traffic between the transit gateways through a peering connection.

Q252. A popular augmented reality (AR) mobile game is heavily using a RESTful API which is hosted in AWS. The API uses Amazon API Gateway and a DynamoDB table with a preconfigured read and write capacity. Based on your systems monitoring, the DynamoDB table begins to throttle requests during high peak loads which causes the slow performance of the game.

Which of the following can you do to improve the performance of your app?

- A. Add the DynamoDB table to an Auto Scaling Group.
- B. Create an SQS queue in front of the DynamoDB table.
- C. Integrate an Application Load Balancer with your DynamoDB table.
- D. Use DynamoDB Auto Scaling

Q253. A new company policy requires IAM users to change their passwords' minimum length to 12 characters. After a random inspection, you found out that there are still employees who do not follow the policy. How can you automatically check and evaluate whether the current password policy for an account complies with the company password policy?

A. Create a Scheduled Lambda Function that will run a custom script to check compliance against changes made to the passwords periodically.

B. Create a CloudTrail trail. Filter the result by setting the attribute to "Event Name" and lookup value to "ChangePassword". This easily gives you the list of users who have made changes to their passwords.

C. Create a rule in the Amazon CloudWatch event. Build an event pattern to match events on IAM. Set the event name to "ChangePassword" in the event pattern. Configure SNS to send notifications to you whenever a user has made changes to his password.

D. Configure AWS Config to trigger an evaluation that will check the compliance for a user's password periodically.

Q254. A company has stored 200 TB of backup files in Amazon S3. The files are in a vendor-proprietary format. The Solutions Architect needs to use the vendor's proprietary file conversion software to retrieve the files from their Amazon S3 bucket, transform the files to an industry-standard format, and re-

upload the files back to Amazon S3. The solution must minimize the data transfer costs. Which of the following options can satisfy the given requirement?

- A. Export the data using AWS Snowball Edge device. Install the file conversion software on the device. Transform the data and re-upload it to Amazon S3.
- B. Deploy the EC2 instance in a different Region. Install the conversion software on the instance. Perform data transformation and re-upload it to Amazon S3.
- C. Install the file conversion software in Amazon S3. Use S3 Batch Operations to perform data transformation.
- D. Deploy the EC2 instance in the same Region as Amazon S3. Install the file conversion software on the instance. Perform data transformation and re-upload it to Amazon S3.

Q255. A web application requires a minimum of six Amazon Elastic Compute Cloud (EC2) instances running at all times. You are tasked to deploy the application to three availability zones in the EU Ireland region (eu-west-1a, eu-west-1b, and eu-west-1c). It is required that the system is fault-tolerant up to the loss of one Availability Zone.

Which of the following setup is the most cost-effective solution which also maintains the fault-tolerance of your system?

- A. 2 instances in eu-west-1a, 2 instances in eu-west-1b, and 2 instances in eu-west-1c

B. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and no instances in eu-west-1c

C. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and 6 instances in eu-west-1c

D. 3 instances in eu-west-1a, 3 instances in eu-west-1b, and 3 instances in eu-west-1c

Q256. The company you are working for has a set of AWS resources hosted in ap-northeast-1 region. You have been asked by your IT Manager to create an AWS CLI shell script that will call an AWS service which could create duplicate resources in another region in the event that ap-northeast-1 region fails. The duplicated resources should also contain the VPC Peering configuration and other networking components from the primary stack.

Which of the following AWS services could help fulfill this task?

A. AWS CloudFormation

B. Amazon LightSail

C. Amazon SNS

D. Amazon SQS

Q257. A technology company is building a new cryptocurrency trading platform that allows the buying and selling of Bitcoin, Ethereum, Ripple, Tether, and many others. You were hired as a Cloud Engineer to build the required

infrastructure needed for this new trading platform. On your first week at work, you started to create

CloudFormation YAML scripts that define all of the needed AWS resources for the application. Your manager was shocked that you haven't created the EC2 instances, S3 buckets, and other AWS resources straight away. He does not understand the text-based scripts that you have done and has asked for your clarification.

In this scenario, what are the benefits of using the Amazon CloudFormation service that you should tell your manager to clarify his concerns? (Select TWO.)

- A. Enables modeling, provisioning, and version-controlling of your entire AWS infrastructure
- B. Allows you to model your entire infrastructure in a text file
- C. A storage location for the code of your application
- D. Provides highly durable and scalable data storage
- E. Using CloudFormation itself is free, including the AWS resources that have been created.

Q258. A data analytics company, which uses machine learning to collect and analyze consumer data, is using Redshift cluster as their data warehouse. You are instructed to implement a disaster recovery plan for their systems to ensure business continuity even in the event of an AWS region outage. Which of the following is the best approach to meet this requirement?

- A. Enable Cross-Region Snapshots Copy in your Amazon Redshift Cluster.
- B. Create a scheduled job that will automatically take the snapshot of your Redshift Cluster and store it to an S3 bucket. Restore the snapshot in case of an AWS region outage.
- C. Use Automated snapshots of your Redshift Cluster.
- D. Do nothing because Amazon Redshift is a highly available, fully-managed data warehouse which can withstand an outage of an entire AWS region.

Q259. A company has a distributed application in AWS that periodically processes large volumes of data across multiple instances. The Solutions Architect designed the application to recover gracefully from any instance failures. He is then required to launch the application in the most cost-effective way. Which type of EC2 instance will meet this requirement?

- A. Dedicated instances
- B. Reserved instances
- C. Spot Instances
- D. On-Demand instances

Q260. A company plans to migrate a NoSQL database to an EC2 instance. The database is configured to replicate the data automatically to keep multiple copies of data for redundancy. The Solutions Architect needs to launch an instance that has a high IOPS and sequential read/write access. Which of the



following options fulfills the requirement if I/O throughput is the highest priority?

- A. Use General purpose instances with EBS volume.
- B. Use Memory optimized instances with EBS volume.
- C. Use Storage optimized instances with instance store volume.
- D. Use Compute optimized instance with instance store volume.

Q261. A company is using an On-Demand EC2 instance to host a legacy web application that uses an Amazon Instance Store-Backed AMI. The web application should be decommissioned as soon as possible and hence, you need to terminate the EC2 instance.

When the instance is terminated, what happens to the data on the root volume?

- A. Data is automatically saved as an EBS snapshot.
- B. Data is unavailable until the instance is restarted.
- C. Data is automatically deleted.
- D. Data is automatically saved as an EBS volume.

Q262. A company is using the AWS Directory Service to integrate their on-premises Microsoft Active Directory (AD) domain with their Amazon EC2 instances via an AD connector. The below identity-based policy is attached to the IAM Identities that use the AWS Directory service:

{

"Version": "2012-10-17",

```
"Statement":[

{

  "Sid":"DirectoryTutorialsDojo1234",

  "Effect":"Allow",

  "Action":[

    "ds:*"

  ],

  "Resource":"arn:aws:ds:us-east-1:987654321012:directory/d-1234567890"11.

}, {

  "Effect":"Allow",

  "Action":[

    "ec2:*"

  ],

  "Resource": "*"

}

]
```

Which of the following BEST describes what the above resource policy does?

A. Allows all AWS Directory Service (ds) calls as long as the resource contains the directory name of:

DirectoryTutorialsDojo1234

B. Allows all AWS Directory Service (ds) calls as long as the resource contains

the directory ID:

987654321012

C. Allows all AWS Directory Service (ds) calls as long as the resource contains

the directory ID:

DirectoryTutorialsDojo1234

D. Allows all AWS Directory Service (ds) calls as long as the resource contains

the directory ID: d- 1234567890

Q263. A company recently launched an e-commerce application that is running in eu-east-2 region, which strictly requires six EC2 instances running at all times. In that region, there are 3 Availability Zones (AZ) that you can use - eu-east-2a, eu-east-2b, and eu-east-2c.

Which of the following deployments provide 100% fault tolerance if any single AZ in the region becomes unavailable? (Select TWO.)

A. eu-east-2a with four EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances

B. eu-east-2a with two EC2 instances, eu-east-2b with four EC2 instances, and eu-east-2c with two EC2 instances

C. eu-east-2a with six EC2 instances, eu-east-2b with six EC2 instances, and eu-east-2c with no EC2 instances

D. eu-east-2a with three EC2 instances, eu-east-2b with three EC2 instances, and eu-east-2c with three EC2 instances

E. eu-east-2a with two EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances

Q264. A newly hired Solutions Architect is checking all of the security groups and network access control list rules of the company's AWS resources. For security purposes, the MS SQL connection via port 1433 of the database tier should be secured. Below is the security group configuration of their Microsoft SQL Server database: The application tier hosted in an Auto Scaling group of EC2 instances is the only identified resource that needs to connect to the database. The Architect should ensure that the architecture complies with the best practice of granting least privilege.

Which of the following changes should be made to the security group configuration?

- A. For the MS SQL rule, change the Source to the Network ACL ID attached to the application tier.
- B. For the MS SQL rule, change the Source to the security group ID attached to the application tier.
- C. For the MS SQL rule, change the Source to the EC2 instance IDs of the underlying instances of the Auto Scaling group.
- D. For the MS SQL rule, change the Source to the static AnyCast IP address attached to the application tier.

Q265. A company has a set of Linux servers running on multiple On-Demand EC2 Instances. The Audit team wants to collect and process the application log files generated from these servers for their report. Which of the following services is best to use in this case?

- A. Amazon S3 Glacier Deep Archive for storing the application log files and AWS ParallelCluster for processing the log files.
- B. Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.
- C. A single On-Demand Amazon EC2 instance for both storing and processing the log files
- D. Amazon S3 Glacier for storing the application log files and Spot EC2 Instances for processing them.

Q266. A startup launched a new FTP server using an On-Demand EC2 instance in a newly created VPC with default settings. The server should not be accessible publicly but only through the IP address 45.116.100 and nowhere else.

Which of the following is the most suitable way to implement this requirement?

- A. Create a new inbound rule in the security group of the EC2 instance with the following details:

Protocol: TCP Port Range: 20 - 21 Source: 175.45.116.100/32

- B. Create a new Network ACL inbound rule in the subnet of the EC2 instance

with the following details:

Protocol: TCP

Port Range: 20 - 21

Source: 175.45.116.100/0

Allow/Deny: ALLOW

C. Create a new Network ACL inbound rule in the subnet of the EC2 instance

with the following details:

Protocol: UDP

Port Range: 20 - 21

Source: 175.45.116.100/0

Allow/Deny: ALLOW

D. Create a new inbound rule in the security group of the EC2 instance with the

following details:

Protocol: UDP

Port Range: 20 - 21

Source: 175.45.116.100/32

Q267. A company is using an Auto Scaling group which is configured to launch new t2.micro EC2 instances when there is a significant load increase in the application. To cope with the demand, you now need to replace those instances with a larger t2.2xlarge instance type. How would you implement this change?

A. Change the instance type of each EC2 instance manually.

- B. Create a new launch configuration with the new instance type and update the Auto Scaling Group.
- C. Just change the instance type to t2.2xlarge in the current launch configuration
- D. Create another Auto Scaling Group and attach the new instance type.

Q268. A company has a two-tier environment in its on-premises data center which is composed of an application tier and database tier. You are instructed to migrate their environment to the AWS cloud, and to design the subnets in their VPC with the following requirements:

1. There is an application load balancer that would distribute the incoming traffic among the servers in the application tier. 2. The application tier and the database tier must not be accessible from the public Internet. The application tier should only accept traffic coming from the load balancer. 3. The database tier contains very sensitive data. It must not share the same subnet with other AWS resources and its 2. custom route table with other instances in the environment. 4. The environment must be highly available and scalable to handle a surge of incoming traffic over the Internet.

3. How many subnets should you create to meet the above requirements?

- A. 4
- B. 6
- C. 3

## D. 2

Q269. A financial firm is designing an application architecture for its online trading platform that must have high availability and fault tolerance. Their Solutions Architect configured the application to use an Amazon S3 bucket located in the us-east-1 region to store large amounts of intraday financial data. The stored financial data in the bucket must not be affected even if there is an outage in one of the Availability Zones or if there's a regional service failure. What should the Architect do to avoid any costly service disruptions and ensure data durability?

- A. Create a Lifecycle Policy to regularly backup the S3 bucket to Amazon Glacier.
- B. Copy the S3 bucket to an EBS-backed EC2 instance.
- C. Create a new S3 bucket in another region and configure Cross-Account Access to the bucket located in us-east-1.
- D. Enable Cross-Region Replication.

Q270. A web application is hosted in an Auto Scaling group of EC2 instances deployed across multiple Availability Zones behind an Application Load Balancer. You need to implement an SSL solution for your system to improve its security which is why you requested an SSL/TLS certificate from a third-party certificate authority (CA).



Where can you safely import the SSL/TLS certificate of your application?

(Select TWO.)

- A. An S3 bucket configured with server-side encryption with customer-provided encryption keys (SSE-C)
- B. AWS Certificate Manager
- C. A private S3 bucket with versioning enabled
- D. CloudFront
- E. IAM certificate store

Q271. A company has a web application hosted in an On-Demand EC2 instance. You are creating a shell script that needs the instance's public and private IP addresses. What is the best way to get the instance's associated IP addresses which your shell script can use?

- A. By using a Curl or Get Command to get the latest metadata information from <http://169.254.169.254/latest/meta-data/>
- B. By using a CloudWatch metric.
- C. By using a Curl or Get Command to get the latest user data information from <http://169.254.169.254/latest/user-data/>
- D. By using IAM.

Q272. A company needs to integrate the Lightweight Directory Access Protocol (LDAP) directory service from the on-premises data center to the AWS VPC

using IAM. The identity store which is currently being used is not compatible with SAML.

Which of the following provides the most valid approach to implement the integration?

- A. Use an IAM policy that references the LDAP identifiers and AWS credentials.
- B. Use AWS Single Sign-On (SSO) service to enable single sign-on between AWS and your LDAP.
- C. Develop an on-premises custom identity broker application and use STS to issue short-lived AWS credentials.
- D. Use IAM roles to rotate the IAM credentials whenever LDAP credentials are updated.

Q273. A company plans to deploy an application in an Amazon EC2 instance.

The application will perform the following tasks:

- Read large datasets from an Amazon S3 bucket.
- Execute multi-stage analysis on the datasets.
- Save the results to Amazon RDS.

During multi-stage analysis, the application will store a large number of temporary files in the instance storage. As the Solutions Architect, you need to recommend the fastest storage option with high I/O performance for the temporary files.

Which of the following options fulfills this requirement?

- A. Configure RAID 1 in multiple instance store volumes.
- B. Attach multiple Provisioned IOPS SSD volumes in the instance.
- C. Configure RAID 0 in multiple instance store volumes.
- D. Enable Transfer Acceleration in Amazon S3.

Q274. A Solutions Architect is working for a large global media company with multiple office locations all around the world. The Architect is instructed to build a system to distribute training videos to all employees. Using CloudFront, what method would be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

- A. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- B. Create a web ACL in AWS WAF to block any public S3 access and attach it to the Amazon CloudFront distribution.
- C. Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM user.
- D. Create an S3 bucket policy that lists the CloudFront distribution ID as the principal and the target bucket as the Amazon Resource Name (ARN).

Q275. A company is looking to store their confidential financial files in AWS which are accessed every week. The Architect was instructed to set up the storage system which uses envelope encryption and automates key rotation. It

should also provide an audit trail that shows who used the encryption key and by whom for security purposes.

Which combination of actions should the Architect implement to satisfy the requirement in the most cost-effective way? (Select TWO.)

- A. Use Amazon S3 Glacier Deep Archive to store the data.
- B. Use Amazon S3 to store the data.
- C. Amazon Certificate Manager
- D. Configure Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
- E. Configure Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). Configure Server-Side Encryption with Customer-Provided Keys (SSE-C).

Q276. A tech startup has recently received a Series A round of funding to continue building their mobile forex trading application. You are hired to set up their cloud architecture in AWS and to implement a highly available, fault tolerant system. For their database, they are using DynamoDB and for authentication, they have chosen to use Cognito. Since the mobile application contains confidential financial transactions, there is a requirement to add a second authentication method that doesn't rely solely on user name and password.

How can you implement this in AWS?

- A. Add a new IAM policy to a user pool in Cognito.
- B. Add multi-factor authentication (MFA) to a user pool in Cognito to protect the identity of your users.
- C. Develop a custom application that integrates with Cognito that implements a second layer of authentication.
- D. Integrate Cognito with Amazon SNS Mobile Push to allow additional authentication via SMS.

Q277. A company has an OLTP (Online Transactional Processing) application that is hosted in an Amazon ECS cluster using the Fargate launch type. It has an Amazon RDS database that stores data of its production website. The Data Analytics team needs to run queries against the database to track and audit all user transactions. These query operations against the production database must not impact application performance in any way.

Which of the following is the MOST suitable and cost-effective solution that you should implement?

- A. Upgrade the instance type of the RDS database to a large instance.
- B. Set up a new Amazon Redshift database cluster. Migrate the product database into Redshift and allow the Data Analytics team to fetch data from it.
- C. Set up a new Amazon RDS Read Replica of the production database. Direct the Data Analytics team to query the production data from the replica.
- D. Set up a Multi-AZ deployments configuration of your production database in

RDS. Direct the Data Analytics team to query the production data from the standby instance.

Q278. A company deployed an online enrollment system database on a prestigious university, which is hosted in RDS. The Solutions Architect is required to monitor the database metrics in Amazon CloudWatch to ensure the availability of the enrollment system.

What are the enhanced monitoring metrics that Amazon CloudWatch gathers from Amazon RDS DB instances which provide more accurate information?

(Select TWO.)

- A. Database Connections
- B. CPU Utilization
- C. RDS child processes.
- D. Freeable Memory
- E. OS processes

Q279. An organization plans to use an AWS Direct Connect connection to establish a dedicated connection between its on-premises network and AWS.

The organization needs to launch a fully managed solution that will automate and accelerate the replication of data to and from various AWS storage services. Which of the following solutions would you recommend?

- A. Use an AWS Storage Gateway file gateway to store and retrieve files directly

using the SMB file system protocol.

B. Use an AWS DataSync agent to rapidly move the data over the Internet.

C. Use an AWS DataSync agent to rapidly move the data over a service endpoint.

D. Use an AWS Storage Gateway tape gateway to store data on virtual tape cartridges and asynchronously copy your backups to AWS.

Q280. A large electronics company is using Amazon Simple Storage Service to store important documents. For reporting purposes, they want to track and log every request access to their S3 buckets including the requester, bucket name, request time, request action, referrer, turnaround time, and error code information. The solution should also provide more visibility into the object-level operations of the bucket. Which is the best solution among the following options that can satisfy the requirement?

A. Enable AWS CloudTrail to audit all Amazon S3 bucket access.

B. Enable server access logging for all required Amazon S3 buckets.

C. Enable the Requester Pays option to track access via AWS Billing.

D. Enable Amazon S3 Event Notifications for PUT and POST.

281. A data analytics company has been building its new generation big data and analytics platform on their AWS cloud infrastructure. They need a storage service that provides the scale and performance that their big data applications

require such as high throughput to compute nodes coupled with read-after-write consistency and low-latency file operations. In addition, their data needs to be stored redundantly across multiple AZs and allows concurrent connections from multiple EC2 instances hosted on multiple AZs. Which of the following AWS storage services will you use to meet this requirement?

- A. Glacier
- B. S3
- C. EBS
- D. EFS

Q282. A company launched an EC2 instance in the newly created VPC. They noticed that the generated instance does not have an associated DNS hostname.

Which of the following options could be a valid reason for this issue?

- A. The newly created VPC has an invalid CIDR block.
- B. The DNS resolution and DNS hostname of the VPC configuration should be enabled.
- C. Amazon Route53 is not enabled.
- D. The security group of the EC2 instance needs to be modified.

Q283. A company has a global news website hosted in a fleet of EC2 Instances. Lately, the load on the website has increased which resulted in slower response



time for the site visitors. This issue impacts the revenue of the company as some readers tend to leave the site if it does not load after 10 seconds. Which of the below services in AWS can be used to solve this problem? (Select TWO.)

- A. Use Amazon ElastiCache for the website's in-memory data store or cache.
- B. Deploy the website to all regions in different VPCs for faster processing.
- C. Use Amazon CloudFront with website as the custom origin.
- D. For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions.

Q284. A leading IT consulting company has an application which processes a large stream of financial data by an Amazon ECS Cluster then stores the result to a DynamoDB table. You have to design a solution to detect new entries in the DynamoDB table then automatically trigger a Lambda function to run some tests to verify the processed data.

What solution can be easily implemented to alert the Lambda function of new entries while requiring minimal configuration change to your architecture?

- A. Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function.
- B. Use CloudWatch Alarms to trigger the Lambda function whenever a new entry is created in the DynamoDB table.
- C. Use Systems Manager Automation to detect new entries in the DynamoDB

table then automatically invoke the Lambda function for processing.

D. Invoke the Lambda functions using SNS each time that the ECS Cluster successfully processed financial data.

Q285. There are a few, easily reproducible but confidential files that your client wants to store in AWS without worrying about storage capacity. For the first month, all of these files will be accessed frequently but after that, they will rarely be accessed at all. The old files will only be accessed by developers so there is no set retrieval time requirement. However, the files under a specific tdojo-finance prefix in the S3 bucket will be used for postprocessing that requires millisecond retrieval time. Given these conditions, which of the following options would be the most cost-effective solution for your client's storage needs?

A. Store the files in S3 then after a month, change the storage class of the tdojo-finance prefix to S3-IA while the remaining go to Glacier using lifecycle policy.

B. Store the files in S3 then after a month, change the storage class of the bucket to S3-IA using lifecycle policy.

C. Store the files in S3 then after a month, change the storage class of the tdojo-finance prefix to One Zone-IA while the remaining go to Glacier using lifecycle policy.

D. Store the files in S3 then after a month, change the storage class of the bucket to Intelligent-Tiering using lifecycle policy.

Q286. To save costs, your manager instructed you to analyze and review the setup of your AWS cloud infrastructure. You should also provide an estimate of how much your company will pay for all of the AWS resources that they are using. In this scenario, which of the following will incur costs? (Select TWO.)

- A. A stopped On-Demand EC2 Instance
- B. Public Data Set
- C. EBS Volumes attached to stopped EC2 Instances
- D. A running EC2 Instance
- E. Using an Amazon VP

Q287. An automotive company is working on an autonomous vehicle development and deployment project using AWS. The solution requires High Performance Computing (HPC) in order to collect, store and manage massive amounts of data as well as to support deep learning frameworks. The Linux EC2 instances that will be used should have a lower latency and higher throughput than the TCP transport traditionally used in cloud-based HPC systems. It should also enhance the performance of inter-instance communication and must include an OSbypass functionality to allow the HPC to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality. Which of the following is the MOST suitable solution that you should implement to achieve the above requirements?

- A. Attach an Elastic Network Interface (ENI) on each Amazon EC2 instance to

accelerate High Performance Computing (HPC).

B. Attach an Elastic Network Adapter (ENA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).

C. Attach a Private Virtual Interface (VIF) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).

D. Attach an Elastic Fabric Adapter (EFA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC).

Q288. A financial company instructed you to automate the recurring tasks in your department such as patch management, infrastructure selection, and data synchronization to improve their current processes. You need to have a service which can coordinate multiple AWS services into serverless workflows. Which of the following is the most cost-effective service to use in this scenario?

A. AWS Step Functions

B. AWS Lambda

C. SWF

D. AWS Batch

Q289. A media company is using Amazon EC2, ELB, and S3 for its video-sharing portal for filmmakers. They are using a standard S3 storage class to store all high-quality videos that are frequently accessed only during the first three months of posting.

As a Solutions Architect, what should you do if the company needs to automatically transfer or archive media data from an S3 bucket to Glacier?

- A. Use Amazon SQS
- B. Use Amazon SWF
- C. Use a custom shell script that transfers data from the S3 bucket to Glacier
- D. Use Lifecycle Policies

Q290. A company recently migrated their applications to AWS. The Solutions Architect must ensure that the applications are highly available and safe from common web security vulnerabilities. Which is the most suitable AWS service to use to mitigate Distributed Denial of Service (DDoS) attacks from hitting your back- end EC2 instances?

- A. AWS WAF
- B. AWS Firewall Manager
- C. AWS Shield
- D. Amazon GuardDuty

Q291. A company plans to develop a custom messaging service that will also be used to train their AI for an automatic response feature which they plan to implement in the future. Based on their research and tests, the service can receive up to thousands of messages a day, and all of these data are to be sent to Amazon EMR for further processing. It is crucial that none of the messages

are lost, no duplicates are produced, and

that they are processed in EMR in the same order as their arrival. Which of the following options can satisfy the given requirement?

- A. Set up an Amazon SNS Topic to handle the messages.
- B. Set up a default Amazon SQS queue to handle the messages.
- C. Create an Amazon Kinesis Data Stream to collect the messages.
- D. Create a pipeline using AWS Data Pipeline to handle the messages.

Q292. A Solutions Architect is migrating several Windows-based applications to AWS that require a scalable file system storage for high-performance computing (HPC). The storage service must have full support for the SMB protocol and Windows NTFS, Active Directory (AD) integration, and Distributed File System (DFS). Which of the following is the MOST suitable storage service that the Architect should use to fulfill this scenario?

- A. Amazon S3 Glacier Deep Archive
- B. Amazon FSx for Windows File Server
- C. AWS DataSync
- D. Amazon FSx for Lustre

Q293. A Solutions Architect is setting up configuration management in an existing cloud architecture. The Architect needs to deploy and manage the EC2 instances including the other AWS resources using Chef and Puppet.

Which of the following is the most suitable service to use in this scenario?

- A. AWS OpsWorks
- B. AWS Elastic Beanstalk
- C. AWS CodeDeploy
- D. AWS CloudFormation

Q294. The start-up company that you are working for has a batch job application that is currently hosted on an EC2 instance. It is set to process messages from a queue created in SQS with default settings. You configured the application to process the messages once a week. After 2 weeks, you noticed that not all messages are being processed by the application. What is the root cause of this issue?

- A. The SQS queue is set to short-polling.
- B. Missing permissions in SQS.
- C. Amazon SQS has automatically deleted the messages that have been in a queue for more than the maximum message retention period.
- D. The batch job application is configured to long polling.

Q295. An organization plans to run an application in a dedicated physical server that doesn't use virtualization. The application data will be stored in a storage solution that uses an NFS protocol. To prevent data loss, you need to use a durable cloud storage service to store a copy of your data. Which of the

following is the most suitable solution to meet the requirement?

A. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure Volume Gateway to store the application data and create an Amazon S3 bucket to store a backup of your data.

B. Use AWS Storage Gateway with a gateway VM appliance for your compute resources.

Configure File Gateway to store the application data and backup data.

C. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure File Gateway to store the application data and create an Amazon S3 bucket to store a backup of your data.

D. Use an AWS Storage Gateway hardware appliance for your compute resources. Configure Volume Gateway to store the application data and backup data.

Q296. A leading media company has recently adopted a hybrid cloud architecture which requires them to migrate their application servers and databases in AWS. One of their applications requires a heterogeneous database

migration in which you need to transform your on-premises Oracle database to PostgreSQL in AWS. This entails a schema and code transformation before the proper data migration starts. Which of the following options is the most suitable approach to migrate the database in AWS?



A. Use Amazon Neptune to convert the source schema and code to match that of the target database in RDS. Use the AWS Batch to effectively migrate the data from the source database to the target database in a batch process.

B. First, use the AWS Schema Conversion Tool to convert the source schema and application code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database.

C. Heterogeneous database migration is not supported in AWS. You have to transform your database first to PostgreSQL and then migrate it to RDS.

D. Configure a Launch Template that automatically converts the source schema and code to match that of the target database. Then, use the AWS Database Migration Service to migrate data from the source database to the target database.

Q297. A company has both on-premises data center as well as AWS cloud infrastructure. They store their graphics, audios, videos, and other multimedia assets primarily in their on-premises storage server and use an S3 Standard storage class bucket as a backup. Their data is heavily used for only a week (7 days) but after that period, it will only be infrequently used by their customers. The Solutions Architect is instructed to save storage costs in AWS yet maintain the ability to

fetch a subset of their media assets in a matter of minutes for a surprise annual data audit, which will be conducted on their cloud storage. Which of the following are valid options that the Solutions Architect can implement to meet the above requirement? (Select TWO.)

- A. Set a lifecycle policy in the bucket to transition the data to S3 Glacier Deep Archive storage class after one week (7 days).
- B. Set a lifecycle policy in the bucket to transition the data to S3 - Standard IA storage class after one week (7 days).
- C. Set a lifecycle policy in the bucket to transition the data to Glacier after one week (7 days).
- D. Set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days
- E. Set a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days).

Q298. A Solutions Architect is working for a fast-growing startup that just started operations during the past 3 months. They currently have an on-premises Active Directory and 10 computers. To save costs in procuring physical workstations, they decided to deploy virtual desktops for their new employees in a virtual private cloud in AWS. The new cloud infrastructure should leverage the existing security controls in AWS but can still communicate with their on-premises network. Which set of AWS services will the Architect use to meet

these requirements?

- A. AWS Directory Services, VPN connection, and Amazon S3
- B. AWS Directory Services, VPN connection, and AWS Identity and Access Management
- C. AWS Directory Services, VPN connection, and ClassicLink
- D. AWS Directory Services, VPN connection, and Amazon Workspaces

Q299. A health organization is using a large Dedicated EC2 instance with multiple EBS volumes to host its health records web application. The EBS volumes must be encrypted due to the confidentiality of the data that they are handling and also to comply with the HIPAA (Health Insurance Portability and Accountability Act) standard.

In EBS encryption, what service does AWS use to secure the volume's data at rest? (Select TWO.)

- A. By using your own keys in AWS Key Management Service (KMS).
- B. By using S3 Server-Side Encryption.
- C. By using the SSL certificates provided by the AWS Certificate Manager (ACM).
- D. By using a password stored in CloudHSM.
- E. By using Amazon-managed keys in AWS Key Management Service (KMS).
- F. By using S3 Client-Side Encryption.

Q300. A multimedia company needs to deploy web services to an AWS region that they have never used before. The company currently has an IAM role for its Amazon EC2 instance that permits the instance to access Amazon DynamoDB. They want their EC2 instances in the new region to have the exact same privileges.

What should be done to accomplish this?

- A. Assign the existing IAM role to instances in the new region.
- B. Duplicate the IAM role and associated policies to the new region and attach it to the instances.
- C. In the new Region, create a new IAM role and associated policies then assign it to the new instance.
- D. Create an Amazon Machine Image (AMI) of the instance and copy it to the new region.

Q301. An On-Demand EC2 instance is launched into a VPC subnet with the Network ACL configured to allow all inbound traffic and deny all outbound traffic. The instance's security group has an inbound rule to allow SSH from any IP address and does not have any outbound rules. In this scenario, what are the changes needed to allow SSH connection to the instance?

- A. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.
- B. No action needed. It can already be accessed from any IP address using

SSH.

C. The network ACL needs to be modified to allow outbound traffic.

D. The outbound security group needs to be modified to allow outbound traffic.

Q302. A data analytics company keeps a massive volume of data that they store in their on-premises data center. To scale their storage systems, they are looking for cloud-backed storage volumes that they can mount using Internet Small Computer System Interface (iSCSI) devices from their on-premises application servers.

They have an on-site data analytics application that frequently accesses the latest data subsets locally while the older data are rarely accessed. You are required to minimize the need to scale the on-premises storage infrastructure while still providing their web application with low-latency access to the data. Which type of AWS Storage Gateway service will you use to meet the above requirements?

A. Volume Gateway in cached mode

B. Volume Gateway in stored mode

C. Tape Gateway

D. File Gateway

Q303. An application is hosted in an Auto Scaling group of EC2 instances. To improve the monitoring process, you have to configure the current capacity to

increase or decrease based on a set of scaling adjustments. This should be done by specifying the scaling metrics and threshold values for the CloudWatch alarms that trigger the scaling process.

Which of the following is the most suitable type of scaling policy that you should use?

- A. Step scaling
- B. Simple scaling
- C. Target tracking scaling
- D. Scheduled Scaling

Q304. A company troubleshoots the operational issues of their cloud architecture by logging the AWS API call history of all AWS resources. The Solutions Architect must implement a solution to quickly identify the most recent changes made to resources in their environment, including creation, modification, and deletion of AWS resources. One of the requirements is that the generated log files should be encrypted to avoid any security issues.

Which of the following is the most suitable approach to implement the encryption?

- A. Use CloudTrail and configure the destination S3 bucket to use Server Side Encryption (SSE) with AES- 128 encryption algorithm.
- B. Use CloudTrail with its default settings
- C. Use CloudTrail and configure the destination Amazon Glacier archive to use

Server-Side Encryption (SSE).

D. Use CloudTrail and configure the destination S3 bucket to use Server-Side Encryption (SSE).

Q305. A company has an infrastructure that allows EC2 instances from a private subnet to fetch objects from Amazon S3 via a NAT Instance. The company's Solutions Architect was instructed to lower down the cost incurred by the current solution.

How should the Solutions Architect redesign the architecture in the most cost-efficient manner?

- A. Remove the NAT instance and create an S3 gateway endpoint to access S3 objects.
- B. Remove the NAT instance and create an S3 interface endpoint to access S3 objects.
- C. Replace the NAT instance with NAT Gateway to access S3 objects.
- D. Use a smaller instance type for the NAT instance.

Q306. An application is hosted on an EC2 instance with multiple EBS Volumes attached and uses Amazon Neptune as its database. To improve data security, you encrypted all of the EBS volumes attached to the instance to protect the confidential data stored in the volumes. Which of the following statements are true about encrypted Amazon Elastic Block Store volumes? (Select TWO.)

- A. Snapshots are automatically encrypted.
- B. All data moving between the volume and the instance are encrypted.
- C. Snapshots are not automatically encrypted.
- D. The volumes created from the encrypted snapshot are not encrypted.
- E. Only the data in the volume is encrypted and not all the data moving between the volume and the instance.

Q307. A Solutions Architect is working for a multinational telecommunications company. The IT Manager wants to consolidate their log streams including the access, application, and security logs in one single system.

Once

consolidated, the company will analyze these logs in real-time based on heuristics. There will be some time in the future where the company will need to validate heuristics, which requires going back to data samples extracted from the last 12 hours.

What is the best approach to meet this requirement?

- A. First, configure Amazon Cloud Trail to receive custom logs and then use EMR to apply heuristics on the logs.
- B. First, send all the log events to Amazon SQS then set up an Auto Scaling group of EC2 servers to consume the logs and finally, apply the heuristics.
- C. First, set up an Auto Scaling group of EC2 servers then store the logs on Amazon S3 then finally, use EMR to apply heuristics on the logs.



D. First, send all of the log events to Amazon Kinesis then afterwards, develop a client process to apply heuristics on the logs.

Q308. A company plans to deploy a Docker-based batch application in AWS. The application will be used to process both mission-critical data as well as non-essential batch jobs. Which of the following is the most costeffective option to use in implementing this architecture?

A. Use ECS as the container management service then set up a combination of Reserved and Spot EC2 Instances for processing mission-critical and non-essential batch jobs respectively.

B. Use ECS as the container management service then set up Reserved EC2 Instances for processing both missioncritical and non-essential batch jobs.

C. Use ECS as the container management service then set up On-Demand EC2 Instances for processing both missioncritical and non-essential batch jobs.

D. Use ECS as the container management service then set up Spot EC2 Instances for processing both mission-critical and non-essential batch jobs.

Q309. A financial analytics application that collects, processes and analyzes stock data in real-time is using

Kinesis Data Streams. The producers continually push data to Kinesis Data Streams while the consumers process the data in real time. In Amazon Kinesis, where can the consumers store their results? (Select TWO.)

- A. Glacier Select
- B. Amazon Athena
- C. Amazon Redshift
- D. Amazon S3
- E. AWS Glue

Q310. A client is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The client also uses Amazon Route 53 to manage their public DNS. How should the client configure the DNS zone apex record to point to the load balancer?

- A. Create an alias for CNAME record to the load balancer DNS name.
- B. Create a CNAME record pointing to the load balancer DNS name.
- C. Create an A record aliased to the load balancer DNS name.
- D. Create an A record pointing to the IP address of the load balancer.

Q311. A company plans to use Route 53 instead of an ELB to load balance the incoming request to the web application. The system is deployed to two EC2 instances to which the traffic needs to be distributed. You want to set a specific percentage of traffic to go to each instance. Which routing policy would you use?

- A. Failover
- B. Weighted

C. Geolocation

D. Latency

Q312. A web application is hosted on an EC2 instance that processes sensitive financial information which is launched in a private subnet. All of the data are stored in an Amazon S3 bucket. Financial information is accessed by users over the Internet. The security team of the company is concerned that the Internet connectivity to Amazon S3 is a security risk.

In this scenario, what will you do to resolve this security vulnerability in the most cost-effective manner?

A. Change the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink.

B. Change the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service.

C. Change the web architecture to access the financial data through a Gateway VPC Endpoint.

D. Change the web architecture to access the financial data in your S3 bucket through a VPN connection.

Q313. A news company is planning to use a Hardware Security Module (CloudHSM) in AWS for secure key storage of their web applications. You have launched the CloudHSM cluster but after just a few hours, a support staff

mistakenly attempted to log in as the administrator three times using an invalid password in the Hardware

Security Module. This has caused the HSM to be zeroized, which means that the encryption keys on it have been wiped. Unfortunately, you did not have a copy of the keys stored anywhere else. How can you obtain a new copy of the keys that you have stored on Hardware Security Module?

- A. Contact AWS Support and they will provide you a copy of the keys.
- B. Restore a snapshot of the Hardware Security Module.
- C. Use the Amazon CLI to get a copy of the keys.
- D. The keys are lost permanently if you did not have a copy.

Q314. A company deployed a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. The Solutions Architect expects the S3 bucket to immediately receive over 2000 PUT requests and 3500 GET requests per second at peak hour.

What should the Solutions Architect do to ensure optimal performance?

- A. Do nothing. Amazon S3 will automatically manage performance at this scale.
- B. Use Byte-Range Fetches to retrieve multiple ranges of an object data per GET request.
- C. Add a random prefix to the key names.
- D. Use a predictable naming scheme in the key names such as sequential numbers or date time sequences.

Q315. A company has 10 TB of infrequently accessed financial data files that would need to be stored in AWS. These data would be accessed infrequently during specific weeks when they are retrieved for auditing purposes. The retrieval time is not strict as long as it does not exceed 24 hours. Which of the following would be a secure, durable, and cost-effective solution for this scenario?

- A. Upload the data to S3 then use a lifecycle policy to transfer data to S3 One Zone-IA.
- B. Upload the data to Amazon FSx for Windows File Server using the Server Message Block (SMB) protocol.
- C. Upload the data to S3 then use a lifecycle policy to transfer data to S3-IA.
- D. Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.

Q316. A company has an On-Demand EC2 instance with an attached EBS volume. There is a scheduled job that creates a snapshot of this EBS volume every midnight at 12 AM when the instance is not used. One night, there has been

a production incident where you need to perform a change on both the instance and on the EBS volume at the same time when the snapshot is currently taking place. Which of the following scenario is true when it comes to the usage of an

EBS volume while the snapshot is in progress?

- A. The EBS volume can be used in read-only mode while the snapshot is in progress.
- B. The EBS volume cannot be used until the snapshot completes.
- C. The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes
- D. The EBS volume can be used while the snapshot is in progress.

Q317. In a startup company you are working for, you are asked to design a web application that requires a NoSQL database that has no limit on the storage size for a given table. The startup is still new in the market and it has very limited human resources who can take care of the database infrastructure. Which is the most suitable service that you can implement that provides a fully managed, scalable and highly available NoSQL service?

- A. SimpleDB
- B. Amazon Neptune
- C. DynamoDB
- D. Amazon Aurora

Q318. A leading e-commerce company is in need of a storage solution that can be simultaneously accessed by 1000 Linux servers in multiple availability zones. The servers are hosted in EC2 instances that use a hierarchical

directory structure via the NFSv4 protocol. The service should be able to handle the rapidly changing data at scale while still maintaining high performance. It should also be highly durable and highly available whenever the servers will pull data from it, with little need for management. As the Solutions Architect, which of the following services is the most cost-effective choice that you should use to meet the above requirement?

- A. EFS
- B. S3
- C. EBS
- D. Storage Gateway

Q319. A company has an application hosted in an Amazon ECS Cluster behind an Application Load Balancer. The Solutions Architect is building a sophisticated web filtering solution that allows or blocks web requests based on the country that the requests originate from. However, the solution should still allow specific IP addresses from that country.

Which combination of steps should the Architect implement to satisfy this requirement? (Select TWO.)

- A. In the Application Load Balancer, create a listener rule that explicitly allows requests from approved IP addresses.
- B. Add another rule in the AWS WAF web ACL with a geo match condition that blocks requests that originate from a specific country.

C. Place a Transit Gateway in front of the VPC where the application is hosted and set up Network ACLs that block requests that originate from a specific country.

D. Using AWS WAF, create a web ACL with a rule that explicitly allows requests from approved IP addresses declared in an IP Set.

E. Set up a geo match condition in the Application Load Balancer that blocks requests from a specific country.

Q320. A company plans to migrate a MySQL database from an on-premises data center to the AWS Cloud. This database will be used by a legacy batch application that has steady-state workloads in the morning but has its peak load at night for the end-of-day processing. You need to choose an EBS volume that can handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance. Which of the following is the most cost-effective storage type to use in this scenario?

A. Amazon EBS Throughput Optimized HDD (st1)

B. Amazon EBS Provisioned IOPS SSD (io1)

C. Amazon EBS General Purpose SSD (gp2)

D. Amazon EBS Cold HDD (sc1)

Q321. A loan processing application is hosted in a single On-Demand EC2 instance in your VPC. To improve the scalability of your application, you have



to use Auto Scaling to automatically add new EC2 instances to handle a surge of incoming requests.

Which of the following items should be done in order to add an existing EC2 instance to an Auto Scaling group? (Select TWO.)

- A. You have to ensure that the instance is launched in one of the Availability Zones defined in your Auto Scaling group.
- B. You must stop the instance first.
- C. You have to ensure that the AMI used to launch the instance still exists.
- D. You have to ensure that the instance is in a different Availability Zone as the Auto Scaling group.
- E. You have to ensure that the AMI used to launch the instance no longer exists.

Q322. An e-commerce application is using a fanout messaging pattern for its order management system. For every order, it sends an Amazon SNS message to an SNS topic, and the message is replicated and pushed to multiple Amazon SQS queues for parallel asynchronous processing. A Spot EC2 instance retrieves the message from each SQS queue and processes the message. There was an incident that while an EC2 instance is currently processing a message, the instance was abruptly terminated, and the processing was not completed in time.

In this scenario, what happens to the SQS message?

- A. The message will be sent to a Dead Letter Queue in AWS DataSync.

B. The message is deleted and becomes duplicated in the SQS when the EC2 instance comes online.

C. When the message visibility timeout expires, the message becomes available for processing by other EC2 instances

D. The message will automatically be assigned to the same EC2 instance when it comes back online within or after the visibility timeout.

Q323. A company needs to use Amazon S3 to store irreproducible financial documents. For their quarterly reporting, the files are required to be retrieved after a period of 3 months. There will be some occasions when a surprise audit will be held, which requires access to the archived data that they need to present immediately.

What will you do to satisfy this requirement in a cost-effective way?

A. Use Amazon S3 Standard

B. Use Amazon S3 Standard - Infrequent Access

C. Use Amazon S3 -Intelligent Tiering

D. Use Amazon Glacier Deep Archive

Q324. A company has a running m5ad.large EC2 instance with a default attached 75 GB SSD instance-store backed volume. You shut it down and then start the instance. You noticed that the data which you have saved earlier on the attached volume is no longer available. What might be the cause of this?

- A. The EC2 instance was using EBS backed root volumes, which are ephemeral and only live for the life of the instance.
- B. The EC2 instance was using instance store volumes, which are ephemeral and only live for the life of the instance.
- C. The volume of the instance was not big enough to handle all of the processing data.
- D. The instance was hit by a virus that wipes out all data.

Q325. A company has several microservices that send messages to an Amazon SQS queue and a backend application that poll the queue to process the messages. The company also has a Service Level Agreement (SLA) which defines the acceptable amount of time that can elapse from the point when the messages are received until a response is sent. The backend operations are I/O-intensive as the number of messages is constantly growing, causing the company to miss its SLA. The Solutions Architect must implement a new architecture that improves the application's processing time and load management. Which of the following is the MOST effective solution that can satisfy the given requirement?

- A. Create an AMI of the backend application's EC2 instance and launch it to a cluster placement group.
- B. Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling group and configure a target tracking scaling policy

based on the CPUUtilization metric with a target value of 80%.

C. Create an AMI of the backend application's EC2 instance and replace it with a larger instance size.

D. Create an AMI of the backend application's EC2 instance. Use the image to set up an Auto Scaling group and configure a target tracking scaling policy based on the ApproximateAgeOfOldestMessage metric.

Q326. A company needs secure access to its Amazon RDS for MySQL database that is used by multiple applications. Each IAM user must use a short-lived authentication token to connect to the database. Which of the following is the most suitable solution in this scenario?

A. Use AWS Secrets Manager to generate and store short-lived authentication tokens.

B. Use an MFA token to access and connect to a database.

C. Use IAM DB Authentication and create database accounts using the AWS-provided AWSAuthenticationPlugin plugin in MySQL.

D. Use AWS SSO to access the RDS database.

Q327. A company has a web application hosted on a fleet of EC2 instances located in two Availability Zones that are all placed behind an Application Load Balancer. As a Solutions Architect, you have to add a health check configuration to ensure your application is highly-available.

Which health checks will you implement?

- A. ICMP health check
- B. FTP health check
- C. HTTP or HTTPS health check
- D. TCP health check

Q328. A startup needs to use a shared file system for its .NET web application running on an Amazon EC2 Windows instance. The file system must provide a high level of throughput and IOPS that can also be integrated with Microsoft Active Directory.

Which is the MOST suitable service that you should use to achieve this requirement?

- A. Amazon FSx for Windows File Server
- B. AWS Storage Gateway - File Gateway
- C. Amazon EBS Provisioned IOPS SSD volumes
- D. Amazon Elastic File System

Q329. A company plans to implement a hybrid architecture. They need to create a dedicated connection from their Amazon Virtual Private Cloud (VPC) to their on-premises network. The connection must provide high bandwidth throughput and a more consistent network experience than Internet-based solutions. Which of the following can be used to create a private connection between the VPC and the company's on- premises network?

- A. Transit VPC
- B. AWS Site-to-Site VPN
- C. AWS Direct Connect
- D. Transit Gateway with equal-cost multipath routing (ECMP)

Q330. A startup launched a fleet of on-demand EC2 instances to host a massively multiplayer online role-playing game (MMORPG). The EC2 instances are configured with Auto Scaling and AWS Systems Manager. What can be used to configure the EC2 instances without having to establish an RDP or SSH connection to each instance?

- A. EC2Config
- B. AWS Config
- C. Run Command
- D. AWS CodePipeline

Q331. An investment bank has a distributed batch processing application which is hosted in an Auto Scaling group of Spot EC2 instances with an SQS queue. You configured your components to use client-side buffering so that the calls made from the client will be buffered first and then sent as a batch request to SQS. What is a period of time during which the SQS queue prevents other consuming components from receiving and processing a message?

- A. Processing Timeout

- B. Receiving Timeout
- C. Component Timeout
- D. Visibility Timeout

Q332. An organization created a new CloudFormation template that creates 4 EC2 instances that are connected to one Elastic Load Balancer (ELB). Which section of the template should be configured to get the Domain Name Server hostname of the ELB upon the creation of the AWS stack?

- A. Resources
- B. Parameters
- C. Mappings
- D. Outputs

Q333. A company is planning to launch a High Performance Computing (HPC) cluster in AWS that does Computational Fluid Dynamics (CFD) simulations. The solution should scale-out their simulation jobs to experiment with more tunable parameters for faster and more accurate results. The cluster is composed of Windows servers hosted on t3a.medium EC2 instances. As the Solutions Architect, you should ensure that the architecture provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies.

Which is the MOST suitable and cost-effective solution that the Architect should

implement to achieve the above requirements?

A. Use AWS ParallelCluster to deploy and manage the HPC cluster to provide higher bandwidth, higher packet per second (PPS) performance, and lower inter-instance latencies.

B. Enable Enhanced Networking with Intel 82599 Virtual Function (VF) interface on the Windows EC2 Instances.

C. Enable Enhanced Networking with Elastic Fabric Adapter (EFA) on the Windows EC2 Instances.

D. Enable Enhanced Networking with Elastic Network Adapter (ENA) on the Windows EC2 Instances.

Q334. A local bank has an in-house application that handles sensitive financial data in a private subnet. After the data is processed by the EC2 worker instances, they will be delivered to S3 for ingestion by other services. How should you design this solution so that the data does not pass through the public Internet?

A. Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3.

B. Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3.

C. Configure a VPC Endpoint along with a corresponding route entry that directs the data to S3.



D. Configure a Transit gateway along with a corresponding route entry that directs the data to S3.

Q335. An online shopping platform is hosted on an Auto Scaling group of On-Demand EC2 instances with a default Auto Scaling termination policy and no instance protection configured. The system is deployed across three Availability Zones in the US West region (us-west-1) with an Application Load Balancer in front to provide high availability and fault tolerance for the shopping platform. The us-west-1a, us-west-1b, and us-west-1c Availability Zones have 10, 8 and 7 running instances respectively. Due to the low number of incoming traffic, the scale-in operation has been triggered. Which of the following will the Auto Scaling group do to determine which instance to terminate first in this scenario? (Select THREE.)

- A. Select the instance that is farthest to the next billing hour.
- B. Select the instance that is closest to the next billing hour.
- C. Select the instances with the most recent launch configuration.
- D. Choose the Availability Zone with the most number of instances, which is the us-west-1a Availability Zone in this scenario.
- E. Choose the Availability Zone with the least number of instances, which is the us-west-1c Availability Zone in this scenario.
- F. Select the instances with the oldest launch configuration.

Q336. An application is hosted in an On-Demand EC2 instance and is using Amazon SDK to communicate to other AWS services such as S3, DynamoDB, and many others. As part of the upcoming IT audit, you need to ensure that all API calls to your AWS resources are logged and durably stored. Which is the most suitable service that you should use to meet this requirement?

- A. Amazon API Gateway
- B. AWS CloudTrail
- C. Amazon CloudWatch
- D. AWS X-Ray

Q337. A company has recently adopted a hybrid cloud architecture and is planning to migrate a database hosted on-premises to AWS. The database currently has over 50 TB of consumer data, handles highly transactional (OLTP) workloads, and is expected to grow. The Solutions Architect should ensure that the database is ACID-compliant and can handle complex queries of the application. Which type of database service should the Architect use?

- A. Amazon RDS
- B. Amazon Redshift
- C. Amazon DynamoDB
- D. Amazon Aurora

Q338. A healthcare company stores sensitive patient health records in their on-

premises storage systems. These records must be kept indefinitely and protected from any type of modifications once they are stored. Compliance regulations mandate that the records must have granular access control and each data access must be audited at all levels. Currently, there are millions of obsolete records that are not accessed by their web application, and their on-premises storage is quickly running out of space. The Solutions Architect must design a solution to immediately move existing records to AWS and support the ever-growing number of new health records.

Which of the following is the most suitable solution that the Solutions Architect should implement to meet the above requirements?

A. Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket.

B. Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Data Events and Amazon S3 Object Lock in the bucket.

C. Set up AWS Storage Gateway to move the existing health records from the on-premises network to the AWS Cloud. Launch an Amazon EBS-backed EC2 instance to store both the existing and new records. Enable Amazon S3 server access logging and S3 Object Lock in the bucket.

D. Set up AWS DataSync to move the existing health records from the on-premises network to the AWS Cloud. Launch a new Amazon S3 bucket to store existing and new records. Enable AWS CloudTrail with Management Events and Amazon S3 Object Lock in the bucket.

Q339. A top IT Consultancy has a VPC with two On-Demand EC2 instances with Elastic IP addresses. You were notified that the EC2 instances are currently under SSH brute force attacks over the Internet. The IT Security team has identified the IP addresses where these attacks originated. You have to immediately implement a temporary fix to stop these attacks while the team is setting up AWS WAF, GuardDuty, and AWS Shield Advanced to permanently fix the security vulnerability. Which of the following provides the quickest way to stop the attacks to the instances?

- A. Remove the Internet Gateway from the VPC
- B. Assign a static Anycast IP address to each EC2 instance
- C. Place the EC2 instances into private subnets
- D. Block the IP addresses in the Network Access Control List

Q340. A web application hosted in an Auto Scaling group of EC2 instances in AWS. The application receives a burst of traffic every morning, and a lot of users are complaining about request timeouts. The EC2 instance takes 1 minute to boot up before it can respond to user requests. The cloud architecture

must be redesigned

to better respond to the changing traffic of the application. How should the Solutions Architect redesign the architecture?

- A. Create a new launch template and upgrade the size of the instance.
- B. Create a step scaling policy and configure an instance warm-up time condition.
- C. Create a CloudFront distribution and set the EC2 instance as the origin.
- D. Create a Network Load Balancer with slow-start mode.

Q341. A Solutions Architect joined a large tech company with an existing Amazon VPC. When reviewing the Auto Scaling events, the Architect noticed that their web application is scaling up and down multiple times within the hour. What design change could the Architect make to optimize cost while preserving elasticity?

- A. Change the cooldown period of the Auto Scaling group and set the CloudWatch metric to a higher threshold
- B. Add provisioned IOPS to the instances
- C. Increase the base number of Auto Scaling instances for the Auto Scaling group
- D. Increase the instance type in the launch configuration

Q342. A data analytics startup is collecting clickstream data and stores them in

an S3 bucket. You need to launch an AWS Lambda function to trigger the ETL jobs to run as soon as new data becomes available in Amazon S3.

Which of the following services can you use as an extract, transform, and load (ETL) service in this scenario?

- A. S3 Select
- B. AWS Glue
- C. Redshift Spectrum
- D. AWS Step Functions

Q343. A company is running a batch job on an EC2 instance inside a private subnet. The instance gathers input data from an S3 bucket in the same region through a NAT Gateway. The company is looking for a solution that will reduce costs without imposing risks on redundancy or availability. Which solution will accomplish this?

- A. Deploy a Transit Gateway to peer connection between the instance and the S3 bucket.
- B. Re-assign the NAT Gateway to a lower EC2 instance type.
- C. Replace the NAT Gateway with a NAT instance hosted on a burstable instance type.
- D. Remove the NAT Gateway and use a Gateway VPC endpoint to access the S3 bucket from the instance.

Q344. A top investment bank is in the process of building a new Forex trading platform. To ensure high availability and scalability, you designed the trading platform to use an Elastic Load Balancer in front of an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones. For its database tier, you chose to use a single Amazon Aurora instance to take advantage of its distributed, fault-tolerant, and self-healing storage system.

In the event of system failure on the primary database instance, what happens to Amazon Aurora during the failover?

A. Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance and is done on a best-effort basis.

B. Aurora will first attempt to create a new DB Instance in a different Availability Zone of the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in the original Availability Zone in which the instance was first launched.

C. Amazon Aurora flips the canonical name record (CNAME) for your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.

D. Amazon Aurora flips the A record of your DB Instance to point at the healthy replica, which in turn is promoted to become the new primary.

Q345. The social media company that you are working for needs to capture the detailed information of all HTTP requests that went through their public-facing

application load balancer every five minutes. They want to use this data for analyzing traffic patterns and for troubleshooting their web applications in AWS.

Which of the following options meet the customer requirements?

- A. Enable Amazon CloudWatch metrics on the application load balancer.
- B. Enable AWS CloudTrail for their application load balancer.
- C. Add an Amazon CloudWatch Logs agent on the application load balancer.
- D. Enable access logs on the application load balancer.

Q346. A company has an application hosted in an Auto Scaling group of Amazon EC2 instances across multiple Availability Zones behind an Application Load Balancer. There are several occasions where some instances are automatically terminated after failing the HTTPS health checks in the ALB and then purges all the ephemeral logs stored in the instance. A Solutions Architect must implement a solution that collects all of the application and server logs effectively. She should be able to perform a root cause analysis based on the logs, even if the Auto Scaling group immediately terminated the instance. What is the EASIEST way for the Architect to automate the log collection from the Amazon EC2 instances?

- A. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances.

Set up AWS Step Functions to collect the application logs and send them to a



CloudWatch Log group.

Configure the solution to resume the instance termination as soon as all the logs were successfully sent to CloudWatch Logs.

B. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of unhealthy Amazon EC2 instances.

Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Trigger the CloudWatch agent to push the application logs and then resume the instance termination once all the logs are sent to CloudWatch Logs.

C. the Pending:Wait state to delay the termination of the unhealthy Amazon EC2 instances.

Configure a CloudWatch Events rule for the EC2 Instance-terminate Lifecycle Action Auto Scaling Event with an associated Lambda function. Set up an AWS Systems Manager Automation script that collects and uploads the application logs from the instance to a CloudWatch Logs group. Configure the solution to only resume the instance termination once all the logs were successfully sent.

D. Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to the Terminating:Wait state to delay the termination of the unhealthy Amazon EC2 instances. Configure a CloudWatch Events rule for the EC2 Instance Terminate Successful Auto Scaling Event with an associated

Lambda function. Set up the AWS Systems Manager Run Command service to run a script that collects and uploads the application logs from the instance to a CloudWatch Logs group.

Resume the instance termination once all the logs are sent.

Q347. A company needs to set up a cost-effective architecture for a log processing application that has frequently accessed, throughput-intensive workloads with large, sequential I/O operations. The application should be hosted in an already existing On-Demand EC2 instance in the VPC. You have to attach a new EBS volume that will be used by the application.

Which of the following is the most suitable EBS volume type that you should use in this scenario?

- A. EBS Throughput Optimized HDD (st1)
- B. EBS General Purpose SSD (gp2)
- C. EBS Provisioned IOPS SSD (io1)
- D. EBS Cold HDD (sc1)

Q348. A company plans to design a highly available architecture in AWS. They have two target groups with three EC2 instances each, which are added to an Application Load Balancer. In the security group of the EC2 instance, you have verified that port 80 for HTTP is allowed. However, the instances are still showing out of service from the load balancer.

What could be the root cause of this issue?

- A. The wrong subnet was used in your VPC
- B. The instances are using the wrong AMI.
- C. The health check configuration is not properly defined.
- D. The wrong instance type was used for the EC2 instance.

Q349. A company has multiple AWS Site-to-Site VPN connections placed between their VPCs and their remote network. During peak hours, many employees are experiencing slow connectivity issues, which limits their productivity. The company has asked a solutions architect to scale the throughput of the VPN connections.

Which solution should the architect carry out?

- A. Add more virtual private gateways to a VPC and enable Equal Cost Multipath Routing (ECMR) to get higher VPN bandwidth.
- B. Associate the VPCs to an Equal Cost Multipath Routing (ECMR)-enabled transit gateway and attach additional VPN tunnels.
- C. Re-route some of the VPN connections to a secondary customer gateway device on the remote network's end.
- D. Modify the VPN configuration by increasing the number of tunnels to scale the throughput.

Q350. A company has a web application hosted in their on-premises infrastructure that they want to migrate to AWS cloud. Your manager has

instructed you to ensure that there is no downtime while the migration process is on-going. In order to achieve this, your team decided to divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure. Once the migration is over and the application works with no issues, a full diversion to AWS will be implemented. The company's VPC is connected to its on-premises network via an AWS Direct Connect connection. Which of the following are the possible solutions that you can implement to satisfy the above requirement? (Select TWO.)

- A. Use an Application Elastic Load balancer with Weighted Target Groups to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- B. Use Route 53 with Failover routing policy to divert and proportion the traffic between the on-premises and AWS-hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.
- C. Use AWS Global Accelerator to divert and proportion the HTTP and HTTPS traffic between the on-premises and AWS-hosted application. Ensure that the on-premises network has an AnyCast static IP address and is connected to your VPC via a Direct Connect Gateway.
- D. Use a Network Load balancer with Weighted Target Groups to divert the traffic between the on-premises and AWS-hosted application. Divert 50% of the

traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.

E. Use Route 53 with Weighted routing policy to divert the traffic between the on-premises and AWS- hosted application. Divert 50% of the traffic to the new application in AWS and the other 50% to the application hosted in their on-premises infrastructure.

Q351. An operations team has an application running on EC2 instances inside two custom VPCs. The VPCs are located in the Ohio and N.Virginia Region respectively. The team wants to transfer data between the instances without traversing the public internet.

Which combination of steps will achieve this? (Select TWO.)

- A. Re-configure the route table's target and destination of the instances' subnet.
- B. Deploy a VPC endpoint on each region to enable a private connection.
- C. Create an Egress-only Internet Gateway.
- D. Set up a VPC peering connection between the VPCs.
- E. Launch a NAT Gateway in the public subnet of each VPC.

Q352. A company plans to design an application that can handle batch processing of large amounts of financial data. The Solutions Architect is tasked to create two Amazon S3 buckets to store the input and output data. The application will transfer the data between multiple EC2 instances over the

network to complete the data processing.

Which of the following options would reduce the data transfer costs?

- A. Deploy the Amazon EC2 instances in private subnets in different Availability Zones.
- B. Deploy the Amazon EC2 instances in the same Availability Zone.
- C. Deploy the Amazon EC2 instances in the same AWS Region.
- D. Deploy the Amazon EC2 instances behind an Application Load Balancer.

Q353. An intelligence agency is currently hosting a learning and training portal in AWS. Your manager instructed you to launch a large EC2 instance with an attached EBS Volume and enable Enhanced Networking. What are the valid case scenarios in using Enhanced Networking? (Select TWO.)

- A. When you need a low packet-per-second performance
- B. When you need a consistently lower inter-instance latencies
- C. When you need a dedicated connection to your on-premises data center
- D. When you need a higher packet per second (PPS) performance
- E. When you need high latency networking

Q354. A company is using Amazon S3 to store frequently accessed data. The S3 bucket is shared with external users that will upload files regularly. A Solutions Architect needs to implement a solution that will grant the bucket owner full access to all uploaded objects in the S3 bucket. What action should

be done to achieve this task?

- A. Enable the Requester Pays feature in the Amazon S3 bucket.
- B. Create a bucket policy that will require the users to set the object's ACL to bucket-owner- full-control.
- C. Create a CORS configuration in the S3 bucket.
- D. Enable server access logging and set up an IAM policy that will require the users to set the object's ACL to bucketowner-full-control.

Q355. A Solutions Architect designed a real-time data analytics system based on Kinesis Data Stream and Lambda. A week after the system has been deployed, the users noticed that it performed slowly as the data rate increases. The Architect identified that the performance of the Kinesis Data Streams is causing this problem.

Which of the following should the Architect do to improve performance?

- A. Replace the data stream with Amazon Kinesis Data Firehose instead.
- B. Implement Step Scaling to the Kinesis Data Stream.
- C. Increase the number of shards of the Kinesis stream by using the UpdateShardCount command.
- D. Improve the performance of the stream by decreasing the number of its shards using the MergeShard command.

Q356. A fast food company is using AWS to host their online ordering system

which uses an Auto Scaling group of EC2 instances deployed across multiple Availability Zones with an Application Load Balancer in front. To better handle the incoming traffic from various digital devices, you are planning to implement a new routing system where requests which have a URL of <server>/api/android are forwarded to one specific target group named "Android-Target-Group". Conversely, requests which have a URL of <server>/api/ios are forwarded to another separate target group named "iOS-Target-Group". How can you implement this change in AWS?

- A. Use path conditions to define rules that forward requests to different target groups based on the URL in the request.
- B. Replace your ALB with a Gateway Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request.
- C. Use host conditions to define rules that forward requests to different target groups based on the hostname in the host header. This enables you to support multiple domains using a single load balancer.
- D. Replace your ALB with a Network Load Balancer then use host conditions to define rules that forward requests to different target groups based on the URL in the request.

Q357. A website hosted on Amazon ECS container instances loads slowly during peak traffic, affecting its availability. Currently, the container instances



are run behind an Application Load Balancer, and CloudWatch alarms are configured to send notifications to the operations team if there is a problem in availability so they can scale out if needed. A solutions architect needs to create an automatic scaling solution when such problems occur.

Which solution could satisfy the requirement? (Select TWO.)

- A. Create an AWS Auto Scaling policy that scales out the ECS cluster when the cluster's CPU utilization is too high.
- B. Create an AWS Auto Scaling policy that scales out the ECS service when the ALB hits a high CPU utilization.
- C. Create an AWS Auto Scaling policy that scales out an ECS service when the ALB endpoint becomes unreachable.
- D. Create an AWS Auto Scaling policy that scales out the ECS service when the service's memory utilization is too high.
- E. Create an AWS Auto Scaling policy that scales out the ECS cluster when the ALB target group's CPU utilization is too high.

Q358. A disaster recovery team is planning to back up on-premises records to a local file server share through SMB protocol. To meet the company's business continuity plan, the team must ensure that a copy of data from 48 hours ago is available for immediate access. Accessing older records with delay is tolerable. Which should the DR team implement to meet the objective with the LEAST amount of configuration effort?

A. Use an AWS Storage File gateway with enough storage to keep data from the last 48 hours.

Send the backups to an SMB share mounted as a local disk.

B. Create an AWS Backup plan to copy data backups to a local SMB share every 48 hours.

C. Mount an Amazon EFS file system on the on-premises client and copy all backups to an NFS share.

D. Create an SMB file share in Amazon FSx for Windows File Server that has enough storage to store all backups. Access the file share from on-premises.

Q359. An application is using a Lambda function to process complex financial data that run for 15 minutes on average. Most invocations were successfully processed. However, you noticed that there are a few terminated invocations throughout the day, which caused data discrepancy in the application. Which of the following is the most likely cause of this issue?

A. The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.

B. The Lambda function contains a recursive code and has been running for over 15 minutes.

C. The concurrent execution limit has been reached.

D. The failed Lambda Invocations contain a ServiceException error which means that the AWS Lambda service encountered an internal error.

Q360. A company's security team requires that all data stored in the cloud be encrypted at rest at all times using encryption keys stored on premises.

Which encryption options meet these requirements? (Select TWO.)

- A. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).
- B. Use server-side encryption with AWS KMS managed encryption keys (SSE-KMS).
- C. Use server-side encryption with customer-provided encryption keys (SSE-C).
- D. Use client-side encryption to provide at-rest encryption.
- E. Use an AWS Lambda function invoked by Amazon S3 events to encrypt the data using the customer's keys.

Q361. A company launched a cryptocurrency mining server on a Reserved EC2 instance in us-east-1 region's private subnet that uses IPv6. Due to the financial data that the server contains, the system should be secured to prevent any unauthorized access and to meet the regulatory compliance requirements. In this scenario, which VPC feature allows the EC2 instance to communicate to the Internet but prevents inbound traffic?

- A. Egress-only Internet gateway
- B. NAT Gateway

C. NAT instances

D. Internet Gateway

Q362. A multinational corporate and investment bank is regularly processing steady workloads of accruals, loan interests, and other critical financial calculations every night from 10 PM to 3 AM on their on-premises data center for their corporate clients. Once the process is done, the results are then uploaded to the Oracle General

Ledger which means that the processing should not be delayed or interrupted. The CTO has decided to move its IT infrastructure to AWS to save costs. The company needs to reserve compute capacity in a specific Availability Zone to properly run their workloads. As the Senior Solutions Architect, how can you implement a cost-effective architecture in AWS for their financial system?

A. Use Dedicated Hosts which provide a physical host that is fully dedicated to running your instances, and bring your existing per-socket, per-core, or per-VM software licenses to reduce costs.

B. Use On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second. Reserve compute capacity in a specific Availability Zone to avoid any interruption.

C. Use Regional Reserved Instances to reserve capacity on a specific Availability Zone and lower down the operating cost through its billing discounts.

D. Use On-Demand Capacity Reservations, which provide compute capacity

that is always available on the specified recurring schedule.

Q363. A Solutions Architect needs to set up the required compute resources for the application which have workloads that require high, sequential read and write access to very large data sets on local storage. Which of the following instance type is the most suitable one to use in this scenario?

- A. Compute Optimized Instances
- B. Memory Optimized Instances
- C. General Purpose Instances
- D. Storage Optimized Instances

Q364. A Solutions Architect is developing a three-tier cryptocurrency web application for a FinTech startup. The Architect has been instructed to restrict access to the database tier to only accept traffic from the application-tier and deny traffic from other sources. The application-tier is composed of application servers hosted in an Auto Scaling group of EC2 instances.

Which of the following options is the MOST suitable solution to implement in this scenario?

- A. Set up the Network ACL of the database subnet to deny all inbound non-database traffic from the subnet of the application-tier.
- B. Set up the security group of the database tier to allow database traffic from a specified list of application server IP addresses.

C. Set up the security group of the database tier to allow database traffic from the security group of the application servers.

D. Set up the Network ACL of the database subnet to allow inbound database traffic from the subnet of the application tier.

Q365. A Solutions Architect needs to launch a web application that will be served globally using Amazon CloudFront. The application is hosted in an Amazon EC2 instance which will be configured as the origin server to process and serve dynamic content to its customers. Which of the following options provides high availability for the application?

A. Launch an Auto Scaling group of EC2 instances and configure it to be part of an origin group.

B. Use Lambda@Edge to improve the performance of your web application and ensure high availability.

Set the Lambda@Edge functions to be part of an origin group.

C. Use Amazon S3 to serve the dynamic content of your web application and configure the S3 bucket to be part of an origin group.

D. Provision two EC2 instances deployed in different Availability Zones and configure them to be part of an origin group.

Q366. A company requires corporate IT governance and cost oversight of all of its AWS resources across its divisions around the world. Their corporate

divisions want to maintain administrative control of the discrete AWS resources they consume and ensure that those resources are separate from other divisions. Which of the following options will support the autonomy of each corporate division while enabling the corporate IT to maintain governance and cost oversight? (Select TWO.)

- A. Use AWS Trusted Advisor and AWS Resource Groups Tag Editor
- B. Create separate VPCs for each division within the corporate IT AWS account. Launch an AWS Transit Gateway with equal-cost multipath routing (ECMP) and VPN tunnels for intra-VPC communication.
- C. Use AWS Consolidated Billing by creating AWS Organizations to link the divisions' accounts to a parent corporate account.
- D. Create separate Availability Zones for each division within the corporate IT AWS account.  
Improve communication between the two AZs using the AWS Global Accelerator.
- E. Enable IAM cross-account access for all corporate IT administrators in each child account.

Q367. A game company has a requirement of load balancing the incoming TCP traffic at the transport level (Layer 4) to their containerized gaming servers hosted in AWS Fargate. To maintain performance, it should handle millions of requests per second sent by gamers around the globe while maintaining ultra-

low latencies. Which of the following must be implemented in the current architecture to satisfy the new requirement?

- A. Launch a new microservice in AWS Fargate that acts as a load balancer since using an ALB or NLB with Fargate is not possible.
- B. Create a new record in Amazon Route 53 with Weighted Routing policy to load balance the incoming traffic.
- C. Launch a new Application Load Balancer.
- D. Launch a new Network Load Balancer.

Q368. A tech company is running two production web servers hosted on Reserved EC2 instances with EBS- backed root volumes. These instances have a consistent CPU load of 90%. Traffic is being distributed to these instances by an Elastic Load Balancer. In addition, they also have Multi-AZ RDS MySQL databases for their production, test, and development environments.

What recommendation would you make to reduce cost in this AWS environment without affecting availability and performance of mission-critical systems?

Choose the best answer.

- A. Consider using On-demand instances instead of Reserved EC2 instances
- B. Consider using Spot instances instead of reserved EC2 instances
- C. Consider not using a Multi-AZ RDS deployment for the development and test database



#### D. Consider removing the Elastic Load Balancer

Q369. A Solutions Architect is managing a three-tier web application that processes credit card payments and online transactions. Static web pages are used on the front-end tier while the application tier contains a single Amazon EC2 instance that handles long-running processes. The data is stored in a MySQL database.

The Solutions Architect is instructed to decouple the tiers to create a highly available application. Which of the following options can satisfy the given requirement?

A. Move all the static assets and web pages to Amazon S3. Re-host the application to Amazon Elastic Container Service (Amazon ECS) containers and enable Service Auto Scaling. Migrate the database to Amazon RDS with Multi-AZ deployments configuration.

B. Move all the static assets, web pages, and the backend application to a larger instance. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon Aurora.

C. Move all the static assets to Amazon S3. Set concurrency limit in AWS Lambda to move the application to a serverless architecture. Migrate the database to Amazon DynamoDB.

D. Move all the static assets and web pages to Amazon CloudFront. Use Auto Scaling in Amazon EC2 instance. Migrate the database to Amazon RDS with

Multi-AZ deployments configuration.

Q370. A company plans to use a cloud storage service to temporarily store its log files. The number of files to be stored is still unknown, but it only needs to be kept for 12 hours. Which of the following is the most cost- effective storage class to use in this scenario?

- A. Amazon S3 Standard-IA
- B. Amazon S3 One Zone-IA
- C. Amazon S3 Standard
- D. Amazon S3 Glacier Deep Archive

Q371. A company created a VPC with a single subnet then launched an On-Demand EC2 instance in that subnet. You have attached an Internet gateway (IGW) to the VPC and verified that the EC2 instance has a public IP.

The main route table of the VPC is as shown below:

However, the instance still cannot be reached from the Internet when you tried to connect to it from your computer. Which of the following should be made to the route table to fix this issue?

- A. Modify the above route table: 10.0.0.0/27 -> Your Internet Gateway
- B. Add the following entry to the route table: 10.0.0.0/27 -> Your Internet Gateway
- C. Add this new entry to the route table: 0.0.0.0/27 -> Your Internet Gateway
- D. Add this new entry to the route table: 0.0.0.0/0 -> Your Internet Gateway

Q372. A large Philippine-based Business Process Outsourcing company is building a two-tier web application in their VPC to serve dynamic transaction-based content. The data tier is leveraging an Online Transactional Processing (OLTP) database but for the web tier, they are still deciding what service they will use. What AWS services should you leverage to build an elastic and scalable web tier?

- A. Amazon RDS with Multi-AZ and Auto Scaling
- B. Elastic Load Balancing, Amazon EC2, and Auto Scaling
- C. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3
- D. Amazon EC2, Amazon DynamoDB, and Amazon S3

Q373. A game development company operates several virtual reality (VR) and augmented reality (AR) games which use various RESTful web APIs hosted on their on-premises data center. Due to the unprecedented growth of their company, they decided to migrate their system to AWS Cloud to scale out their resources as well to minimize costs.

Which of the following should you recommend as the most cost-effective and scalable solution to meet the above requirement?

- A. Use AWS Lambda and Amazon API Gateway.
- B. Set up a micro-service architecture with ECS, ECR, and Fargate.
- C. Use a Spot Fleet of Amazon EC2 instances, each with an Elastic Fabric Adapter (EFA) for more consistent latency and higher network throughput. Set up an Application Load Balancer to distribute traffic to the instances.
- D. Host the APIs in a static S3 web hosting bucket behind a CloudFront web distribution.

Q374. A computer animation film studio has a web application running on an Amazon EC2 instance. It uploads 5 GB video objects to an Amazon S3 bucket. Video uploads are taking longer than expected, which impacts the performance of your application.

Which method will help improve the performance of the application?

- A. Leverage on Amazon CloudFront and use HTTP POST method to reduce

latency.

B. Use Amazon S3 Multipart Upload API.

C. Enable Enhanced Networking with the Elastic Network Adapter (ENA) on your EC2 Instances.

D. Use Amazon Elastic Block Store Provisioned IOPS and an Amazon EBS-optimized instance.

Q375. A company deployed a web application to an EC2 instance that adds a variety of photo effects to a picture uploaded by the users. The application will put the generated photos to an S3 bucket by sending PUT requests to the S3 API.

What is the best option for this scenario considering that you need to have API credentials to be able to send a request to the S3 API?

A. Encrypt the API credentials and store in any directory of the EC2 instance.

B. Store the API credentials in the root web application directory of the EC2 instance.

C. Store your API credentials in Amazon Glacier.

D. Create a role in IAM. Afterwards, assign this role to a new EC2 instance.

Q376. A company has an application that uses multiple EC2 instances located in various AWS regions such as US

East (Ohio), US West (N. California), and EU (Ireland). The manager instructed

the Solutions Architect to set up a latency-based routing to route incoming traffic for [www.tutorialsdojo.com](http://www.tutorialsdojo.com) to all the EC2 instances across all AWS regions.

Which of the following options can satisfy the given requirement?

- A. Use a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.
- B. Use AWS DataSync to distribute the load to the multiple EC2 instances across all AWS Regions.
- C. Use an Application Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.
- D. Use Route 53 to distribute the load to the multiple EC2 instances across all AWS Regions.

Q377. A commercial bank has designed its next-generation online banking platform to use a distributed system architecture. As their Software Architect, you have to ensure that their architecture is highly scalable, yet still cost-effective. Which of the following will provide the most suitable solution for this scenario?

- A. Launch an Auto-Scaling group of EC2 instances to host your application services and an SQS queue. Include an Auto Scaling trigger to watch the SQS queue size which will either scale in or scale out the number of EC2 instances based on the queue.
- B. Launch multiple On-Demand EC2 instances to host your application services

and an SQS queue which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

C. Launch multiple EC2 instances behind an Application Load Balancer to host your application services, and SWF which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

D. Launch multiple EC2 instances behind an Application Load Balancer to host your application services and SNS which will act as a highly-scalable buffer that stores messages as they travel between distributed applications.

Q378. A software development company needs to connect its on-premises infrastructure to the AWS cloud. Which of the following AWS services can you use to accomplish this? (Select TWO.)

- A. NAT Gateway
- B. VPC Peering
- C. IPsec VPN connection
- D. AWS Direct Connect
- E. Amazon Connect

Q379. A web application is hosted on a fleet of EC2 instances inside an Auto Scaling Group with a couple of Lambda functions for ad hoc processing. Whenever you release updates to your application every week, there are inconsistencies where some resources are not updated properly. You need a

way to group the resources together and deploy the new version of your code consistently among the groups with minimal downtime.

Which among these options should you do to satisfy the given requirement with the least effort?

- A. Use CodeCommit to publish your code quickly in a private repository and push them to your resources for fast updates.
- B. Use deployment groups in CodeDeploy to automate code deployments in a consistent manner.
- C. Create CloudFormation templates that have the latest configurations and code in them.
- D. Create OpsWorks recipes that will automatically launch resources containing the latest version of the code.

Q380. A company is using an Amazon RDS for MySQL 5.6 with Multi-AZ deployment enabled and several web servers across two AWS Regions. The database is currently experiencing highly dynamic reads due to the growth of the company's website. The Solutions Architect tried to test the read performance from the secondary AWS Region and noticed a notable slowdown on the SQL queries. Which of the following options would provide a read replication latency of less than 1 second?

- A. Use Amazon ElastiCache to improve database performance.
- B. Migrate the existing database to Amazon Aurora and create a cross-region



read replica.

C. Create an Amazon RDS for MySQL read replica in the secondary AWS Region.

D. Upgrade the MySQL database engine.

Q381. A construction company has an online system that tracks all of the status and progress of their projects. The system is hosted in AWS and there is a requirement to monitor the read and write IOPs metrics for their MySQL RDS instance and send real-time alerts to their DevOps team. Which of the following services in AWS can you use to meet the requirements? (Select TWO.)

A. Amazon Simple Queue Service

B. CloudWatch

C. Route 53

D. SWF

E. Amazon Simple Notification Service

Q382. A company has several EC2 Reserved Instances in their account that need to be decommissioned and shut down since they are no longer used by the development team. However, the data is still required by the audit team for compliance purposes.

Which of the following steps can be taken in this scenario? (Select TWO.)

A. Stop all the running EC2 instances.

- B. Convert the EC2 instance to On-Demand instances
- C. Take snapshots of the EBS volumes and terminate the EC2 instances.
- D. You can opt to sell these EC2 instances on the AWS Reserved Instance Marketplace
- E. Convert the EC2 instances to Spot instances with a persistent Spot request type.

Q383. A top university has recently launched its online learning portal where the students can take e-learning courses from the comforts of their homes. The portal is on a large On-Demand EC2 instance with a single Amazon Aurora database.

How can you improve the availability of your Aurora database to prevent any unnecessary downtime of the online portal?

- A. Use an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes.
- B. Enable Hash Joins to improve the database query performance.
- C. Deploy Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing.
- D. Create Amazon Aurora Replicas.

Q384. A global news network created a CloudFront distribution for their web application. However, you noticed that the application's origin server is being

hit for each request instead of the AWS Edge locations, which serve the cached objects. The issue occurs even for the commonly requested objects. What could be a possible cause of this issue?

- A. The file sizes of the cached objects are too large for CloudFront to handle.
- B. An object is only cached by Cloudfront once a successful request has been made hence, the objects were not requested before, which is why the request is still directed to the origin server.
- C. There are two primary origins configured in your Amazon CloudFront Origin Group.
- D. The Cache-Control max-age directive is set to zero.

Q385. A startup is building IoT devices and monitoring applications. They are using IoT sensors to monitor the traffic in real-time by using an Amazon Kinesis Stream that is configured with default settings. It then sends the data to an Amazon S3 bucket every 3 days. When you checked the data in S3 on the 3rd day, only the data for the last day is present and no data is present from 2 days ago. Which of the following is the MOST likely cause of this issue?

- A. Someone has manually deleted the record in Amazon S3.
- B. Amazon S3 bucket has encountered a data loss.
- C. The access of the Kinesis stream to the S3 bucket is insufficient.
- D. By default, data records in Kinesis are only accessible for 24 hours from the time they are added to a stream.

Q386. A Solutions Architect is implementing a new High-Performance Computing (HPC) system in AWS that involves orchestrating several Amazon Elastic Container Service (Amazon ECS) tasks with an EC2 launch type that is part of an Amazon ECS cluster. The system will be frequently accessed by users around the globe and it is expected that there would be hundreds of ECS tasks running most of the time. The Architect must ensure that its storage system is optimized for high-frequency read and write operations. The output data of each ECS task is around 10 MB but the obsolete data will eventually be archived and deleted so the total storage size won't exceed 10 TB.

Which of the following is the MOST suitable solution that the Architect should recommend?

A. Launch an Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode and set the performance mode to General Purpose. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster.

B. Launch an Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode and set the performance mode to Max I/O. Configure the EFS file system as the container mount point in the ECS task definition of the Amazon ECS cluster.

C. Launch an Amazon DynamoDB table with Amazon DynamoDB Accelerator (DAX) and DynamoDB Streams enabled. Configure the table to be accessible

by all Amazon ECS cluster instances. Set the DynamoDB table as the container mount point in the ECS task definition of the Amazon ECS cluster.

D. Set up an SMB file share by creating an Amazon FSx File Gateway in Storage Gateway. Set the file share as the container mount point in the ECS task definition of the Amazon ECS cluster.

Q387. A company has a fleet of running Spot EC2 instances behind an Application Load Balancer. The incoming traffic comes from various users across multiple AWS regions and you would like to have the user's session shared among the fleet of instances. You are required to set up a distributed session management layer that will provide a scalable and shared data storage for the user sessions. Which of the following would be the best choice to meet the requirement while still providing sub- millisecond latency for the users?

- A. Multi-AZ RDS
- B. Elastic ache in-memory caching
- C. Multi-master DynamoDB
- D. ELB sticky sessions

Q388. A company is planning to deploy a High Performance Computing (HPC) cluster in its VPC that requires a scalable, high-performance file system. The storage service must be optimized for efficient workload processing, and the

data must be accessible via a fast and scalable file system interface. It should also work

natively with Amazon S3 that enables you to easily process your S3 data with a high-performance POSIX interface.

Which of the following is the MOST suitable service that you should use for this scenario?

- A. Amazon Elastic File System (EFS)
- B. Amazon Elastic Block Storage (EBS)
- C. Amazon FSx for Lustre
- D. Amazon FSx for Windows File Server

Q389. A Solutions Architect created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to Amazon S3, DynamoDB, Lambda, and other AWS resources of the company's cloud infrastructure.

Which of the following must be done to allow the user to make API calls to the AWS resources?

- A. Do nothing as the IAM User is already capable of sending API calls to your AWS resources.
- B. Enable Multi-Factor Authentication for the user.
- C. Create a set of Access Keys for the user and attach the necessary

permissions.

D. Assign an IAM Policy to the user to allow it to send API calls.

Q390. A company plans to implement a network monitoring system in AWS. The Solutions Architect launched an EC2 instance to host the monitoring system and used CloudWatch to monitor, store, and access the log files of the instance.

Which of the following provides an automated way to send log data to CloudWatch Logs from the Amazon EC2 instance?

- A. AWS Transfer for SFTP
- B. CloudTrail with log file validation
- C. CloudWatch Logs agent
- D. CloudTrail Processing Library

Q391. A cryptocurrency company wants to go global with its international money transfer app. Your project is to make sure that the database of the app is highly available in multiple regions. What are the benefits of adding Multi-AZ deployments in Amazon RDS? (Select TWO.)

- A. Provides SQL optimization.
- B. Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.
- C. Provides enhanced database durability in the event of a DB instance

component failure or an Availability Zone outage.

D. Significantly increases the database performance.

E. Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region.

Q392. A company has an application architecture that stores both the access key ID and the secret access key in a plain text file on a custom Amazon Machine Image (AMI). The EC2 instances, which are created by using this AMI, are using the stored access keys to connect to a DynamoDB table. What should the Solutions Architect do to make the current architecture more secure?

A. Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image.

B. Remove the stored access keys in the AMI. Create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.

C. Put the access keys in an Amazon S3 bucket instead.

D. Put the access keys in Amazon Glacier instead.

Q393. A tech company is having an issue whenever they try to connect to the newly created EC2 instance using a Remote Desktop connection from a computer. Upon checking, the Solutions Architect has verified that the instance has a public IP and the Internet gateway and route tables are in place. What else should he do to resolve



this issue?

- A. You should restart the EC2 instance since there might be some issue with the instance
- B. Adjust the security group to allow inbound traffic on port 3389 from the company's IP address.
- C. Adjust the security group to allow inbound traffic on port 22 from the company's IP address.
- D. You should create a new instance since there might be some issue with the instance

Q394. A Solutions Architect is working for a weather station in Asia with a weather monitoring system that needs to be migrated to AWS. Since the monitoring system requires a low network latency and high network throughput, the Architect decided to launch the EC2 instances to a new cluster placement group. The system was working fine for a couple of weeks, however, when they try to add new instances to the placement group that already has running EC2 instances, they receive an 'insufficient capacity error'. How will the Architect fix this issue?

- A. Stop and restart the instances in the Placement Group and then try the launch again.
- B. Verify all running instances are of the same size and type and then try the launch again.

C. Create another Placement Group and launch the new instances in the new group.

D. Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group.

Q395. There is a technical requirement by a financial firm that does online credit card processing to have a secure application environment on AWS. They are trying to decide on whether to use KMS or CloudHSM. Which of the following statements is right when it comes to Cloud HSM and KMS?

A. If you want a managed service for creating and controlling your encryption keys but don't want or need to operate your own HSM, consider using AWS Cloud HSM.

B. AWS Cloud HSM should always be used for any payment transactions.

C. You should consider using AWS Cloud HSM over AWS KMS if you require your keys stored in dedicated, thirdparty validated hardware security modules under your exclusive control.

D. No major difference. They both do the same thing.

Q396. A manufacturing company launched a new type of IoT sensor. The sensor will be used to collect large streams of data records. You need to create a solution that can ingest and analyze the data in real-time with millisecond response times.

Which of the following is the best option that you should implement in this scenario?

- A. Ingest the data using Amazon Simple Queue Service and create an AWS Lambda function to store the data in Amazon Redshift.
- B. Ingest the data using Amazon Kinesis Data Firehose and create an AWS Lambda function to store the data in Amazon DynamoDB.
- C. Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon DynamoDB.
- D. Ingest the data using Amazon Kinesis Data Streams and create an AWS Lambda function to store the data in Amazon Redshift.

Q397. A software development company has hundreds of Amazon EC2 instances with multiple Application

Load Balancers (ALBs) across multiple AWS Regions. The public applications hosted in their EC2 instances are accessed on their on-premises network. The company needs to reduce the number of IP addresses that it needs to regularly whitelist on the corporate firewall device. Which of the following approach can be used to fulfill this requirement?

- A. Create a new Lambda function that tracks the changes in the IP addresses of all ALBs across multiple AWS Regions. Schedule the function to run and update the corporate firewall every hour using Amazon CloudWatch Events.
- B. Use AWS Global Accelerator and create an endpoint group for each AWS

Region. Associate the Application Load Balancer from each region to the corresponding endpoint group.

C. Use AWS Global Accelerator and create multiple endpoints for all the available AWS Regions.

Associate all the private IP addresses of the EC2 instances to the corresponding endpoints.

D. Launch a Network Load Balancer with an associated Elastic IP address. Set the ALBs in multiple Regions as targets.

Q398. A Solutions Architect needs to create a publicly accessible EC2 instance by using an Elastic IP (EIP) address and generate a report on how much it will cost to use that EIP. Which of the following statements is correct regarding the pricing of EIP?

A. There is no cost if the instance is running and it has only one associated EIP.

B. There is no cost if the instance is terminated and it has only one associated EIP.

C. There is no cost if the instance is running and it has at least two associated EIP.

D. There is no cost if the instance is stopped and it has only one associated EIP.

Q399. A startup is building a microservices architecture in which the software

is composed of small independent services that communicate over well-defined APIs. In building large-scale systems, fine-grained decoupling of microservices is a recommended practice to implement. The decoupled services should scale horizontally from each other to improve scalability.

What is the difference between Horizontal scaling and Vertical scaling?

A. Vertical scaling means running the same software on a fully serverless architecture using Lambda.

Horizontal scaling means adding more servers to the existing pool and it doesn't run into limitations of individual servers.

B. Horizontal scaling means running the same software on smaller containers such as Docker and Kubernetes using ECS or EKS. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

C. Horizontal scaling means running the same software on bigger machines which is limited by the capacity of individual servers. Vertical scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

D. Vertical scaling means running the same software on bigger machines which is limited by the capacity of the individual server. Horizontal scaling is adding more servers to the existing pool and doesn't run into limitations of individual servers.

Q400. A new DevOps engineer has created a CloudFormation template for a web application and she raised a `pull request` in GIT for you to check and review. After checking the template, you immediately told her that the template will not work. Which of the following is the reason why this CloudFormation template will fail to deploy the stack?

```
{  "AWSTemplateFormatVersion":"2010-09-09",  "Parameters":{    "VPCId":{      "Type":"String",      "Description":"manila"    },    "SubnetId":{      "Type":"String",      "Description":"subnet-b46032ec"    },    "Outputs":{      "InstanceId":{        "Value":{          "Ref":"manilaInstance"        },        "Description":"Instance Id"      }    }  }
```

- A. The Resources section is missing.
- B. The Conditions section is missing.
- C. An invalid section named Parameters is present. This will cause the CloudFormation stack to fail.
- D. The value of the AWSTemplateFormatVersion is incorrect. It should be 2017-06-06.

Q401. An online shopping platform has been deployed to AWS using Elastic Beanstalk. They simply uploaded their Node.js application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring. Since the entire deployment process is automated, the DevOps team is not sure where to get the application log files of their shopping platform. In Elastic Beanstalk, where

does it store the application files and server log files?

A. Application files are stored in S3. The server log files can only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk.

B. Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.

C. Application files are stored in S3. The server log files can be stored directly in Glacier or in CloudWatch Logs.

D. Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs.

Q402. A Solutions Architect is trying to enable Cross-Region Replication to an S3 bucket but this option is disabled. Which of the following options is a valid reason for this?

A. In order to use the Cross-Region Replication feature in S3, you need to first enable versioning on the bucket.

B. The Cross-Region Replication feature is only available for Amazon S3 One Zone-IA•

C. The Cross-Region Replication feature is only available for Amazon S3 Infrequent Access.•

D. This is a premium feature which is only for AWS Enterprise accounts.

Q403. An online stock trading system is hosted in AWS and uses an Auto Scaling group of EC2 instances, an RDS database, and an Amazon ElastiCache for Redis. You need to improve the data security of your in-memory data store by requiring the user to enter a password before they are granted permission to execute Redis commands.

Which of the following should you do to meet the above requirement?

- A. Do nothing. This feature is already enabled by default.
- B. Enable the in-transit encryption for Redis replication groups.
- C. Create a new Redis replication group and set the `AtRestEncryptionEnabled` parameter to true.
- D. None of the above.
- E. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the `--transit-encryption-enabled` and `--auth-token` parameters enabled.

Q404. A mobile application stores pictures in Amazon Simple Storage Service (S3) and allows application sign-in using an OpenID Connect-compatible identity provider. Which AWS Security Token Service approach to temporary access should you use for this scenario?

- A. SAML-based Identity Federation
- B. Web Identity Federation
- C. Cross-Account Access



## D. AWS Identity and Access Management roles

Q405. A web application, which is hosted in your on-premises data center and uses a MySQL database, must be migrated to AWS Cloud. You need to ensure that the network traffic to and from your RDS database instance is encrypted using SSL. For improved security, you have to use the profile credentials specific to your EC2 instance to access your database, instead of a password. Which of the following should you do to meet the above requirement?

- A. Launch a new RDS database instance with the Backtrack feature enabled.
- B. Set up an RDS database and enable the IAM DB Authentication.
- C. Configure your RDS database to enable encryption.
- D. Launch the mysql client using the --ssl-ca parameter when connecting to the database.

Q406. A company has several unencrypted EBS snapshots in their VPC. The Solutions Architect must ensure that all of the new EBS volumes restored from the unencrypted snapshots are automatically encrypted. What should be done to accomplish this requirement?

- A. Enable the EBS Encryption By Default feature for the AWS Region.
- B. Enable the EBS Encryption By Default feature for specific EBS volumes.
- C. Launch new EBS volumes and encrypt them using an asymmetric customer

master key (CMK).

D. Launch new EBS volumes and specify the symmetric customer master key (CMK) for encryption.

Q407. An application is hosted in an Auto Scaling group of EC2 instances and a Microsoft SQL Server on Amazon RDS. There is a requirement that all in-flight data between your web servers and RDS should be secured. Which of the following options is the MOST suitable solution that you should implement? (Select TWO.)

A. Force all connections to your DB instance to use SSL by setting the `rds.force_ssl` parameter to true.

Once done, reboot your DB instance.

B. Download the Amazon RDS Root CA certificate. Import the certificate to your servers and configure your application to use SSL to encrypt the connection to RDS.

C. Enable the IAM DB authentication in RDS using the AWS Management Console.

D. Configure the security groups of your EC2 instances and RDS to only allow traffic to and from port 443.

E. Specify the TDE option in an RDS option group that is associated with that DB instance to enable transparent data encryption (TDE).

Q408. In a tech company that you are working for, there is a requirement to allow one IAM user to modify the configuration of one of your Elastic Load Balancers (ELB) which is used in a specific project. Each developer in your company has an individual IAM user and they usually move from one project to another. Which of the following would be the best way to allow this access?

- A. Provide the user temporary access to the root account for 8 hours only. Afterwards, change the password once the activity is completed.
- B. Create a new IAM user that has access to modify the ELB. Delete that user when the work is completed.
- C. Open up the port that ELB uses in a security group and then give the user access to that security group via a policy.
- D. Create a new IAM Role which will be assumed by the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role from the user.

Q409. A startup is building an AI-based face recognition application in AWS, where they store millions of images in an S3 bucket. As the Solutions Architect, you have to ensure that each and every image uploaded to their system is stored without any issues.

What is the correct indication that an object was successfully stored when you put objects in Amazon S3?

- A. You will receive an email from Amazon SNS informing you that the object is

successfully stored.

B. Amazon S3 has 99.999999999% durability hence, there is no need to confirm that data was inserted.

C. You will receive an SMS from Amazon SNS informing you that the object is successfully stored.

D. HTTP 200 result code and MD5 checksum.

Q410. A company has a VPC for its human resource department, and another VPC located in a different region for their finance department. The Solutions Architect must redesign the architecture to allow the finance department to access all resources that are in the human resource department, and vice versa. Which type of networking connection in AWS should the Solutions Architect set up to satisfy the above requirement?

A. VPN Connection

B. AWS Cloud Map

C. VPC Endpoint

D. Inter-Region VPC Peering

Q411. A company plans to launch an application that tracks the GPS coordinates of delivery trucks in the country. The coordinates are transmitted from each delivery truck every five seconds. You need to design an architecture that will enable real-time processing of these coordinates from multiple

consumers. The aggregated data will be analyzed in a separate reporting application.

Which AWS service should you use for this scenario?

- A. Amazon Simple Queue Service
- B. Amazon Kinesis
- C. Amazon AppStream
- D. AWS Data Pipeline

Q412. A company deployed a fleet of Windows-based EC2 instances with IPv4 addresses launched in a private subnet. Several software installed in the EC2 instances are required to be updated via the Internet. Which of the following services can provide the firm a highly available solution to safely allow the instances to fetch the software patches from the Internet but prevent outside network from initiating a connection?

- A. VPC Endpoint
- B. NAT Gateway
- C. NAT Instance
- D. Egress-Only Internet Gateway

Q413. A company developed a financial analytics web application hosted in a Docker container using MEAN (MongoDB, Express.js, AngularJS, and Node.js) stack. You want to easily port that web application to AWS Cloud which can

automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster.

Which of the following services can be used to fulfill this requirement?

- A. OpsWorks
- B. ECS
- C. AWS Elastic Beanstalk
- D. AWS Code Deploy