

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Correct Answer: B

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Correct Answer: A

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world.

Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance. What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: C

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Correct Answer: *B*

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Correct Answer: *D*

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Correct Answer: *BD*

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Choose two.)

- A. Add AWS Shield.
- B. Add Aurora Replica.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Correct Answer: DE

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Correct Answer: C

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity.
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Correct Answer: C

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for

certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Correct Answer: C

A company is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones.

The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Correct Answer: B

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Correct Answer: C

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. EBS Amazon Elastic Block Store (Amazon EBS)

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

Correct Answer: *B*

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Correct Answer: *D*

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Correct Answer: *BC*

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Correct Answer: C

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customizations. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customizations. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customizations. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customizations. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Correct Answer: B

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Correct Answer: C

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

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

Correct Answer: B

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Correct Answer: A

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

- A. Amazon S3 for cold data storage
- B. Amazon Elastic File System (Amazon EFS) for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Correct Answer: BD

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.

What should the solutions architect do to accomplish this? (Choose two.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Correct Answer: AB

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Correct Answer: C

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon Elastic Block Store (Amazon EBS).
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon Elastic File System (Amazon EFS).
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Correct Answer: D

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.

Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Correct Answer: A

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions.
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Correct Answer: C

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances

Correct Answer: D

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.

What should a solutions architect do to meet these requirements? (Choose two.)?

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.

- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Correct Answer: *CE*

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Correct Answer: *C*

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Correct Answer: *C*

A solutions architect has created a new AWS account and must secure AWS account root user access.

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

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: *AB*

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: *B*

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Correct Answer: *B*

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Correct Answer: *C*

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Correct Answer: C

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage. There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly when the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Correct Answer: D

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: A

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database

hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.

Which changes should be made to the database tier to improve performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
- C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Correct Answer: *D*

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution. What should a solutions architect do to accomplish this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
- D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Correct Answer: *B*

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1)

Correct Answer: *B*

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions

architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.

What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
- B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.
- C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Correct Answer: A

A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

- A. Enable Amazon S3 versioning.
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy.
- D. Enable Amazon S3 cross-Region replication.

Correct Answer: A

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Correct Answer: B

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meets these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.

- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Correct Answer: *B*

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon Elastic Block Store (Amazon EBS) volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

- A. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
- B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon Elastic File System (Amazon EFS) and mount a target on each instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: *C*

A security team to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations.

The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Correct Answer: *D*

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.

What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: *B*

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon Elastic Block Store (Amazon EBS) volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon Elastic File System (Amazon EFS). Modify the application to save new documents to Amazon Elastic File System (Amazon EFS).
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Correct Answer: C

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Correct Answer: D

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Correct Answer: D

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A

solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

- A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.
- B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
- C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.
- E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Correct Answer: *DE*

A solutions architect is tasked with transferring 750 TB of data from an on-premises network-attached file system located at a branch office Amazon S3 Glacier.

The migration must not saturate the on-premises 1 Mbps internet connection.

Which solution will meet these requirements?

- A. Create an AWS site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Transfer the files directly by using the AWS CLI.
- B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to an S3 bucket, and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- D. Order 10 AWS Snowball Edge Storage Optimized devices, and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Correct Answer: *D*

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Choose two.)

- A. Create new public and private subnets in the same AZ for high availability.
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.
- E. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Correct Answer: *BE*

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: *BD*

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.

What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Correct Answer: *C*

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: *AC*

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.

- B. Use service control policies to disable IAM activity across all accounts in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Correct Answer: *D*

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: *B*

A company runs an application on a group of Amazon Linux EC2 instances. For compliance reasons, the company must retain all application log files for 7 years.

The log files will be analyzed by a reporting tool that must access all files concurrently.

Which storage solution meets these requirements MOST cost-effectively?

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

Correct Answer: *D*

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Correct Answer: *C*

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an

Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.

What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Correct Answer: A

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
- D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

Correct Answer: C

A company has on-premises servers that run a relational database. The database serves high-read traffic for users in different locations. The company wants to migrate the database to AWS with the least amount of effort. The database solution must support high availability and must not affect the company's current traffic flow. Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.
- C. Use databases that are hosted on multiple Amazon EC2 instances in different AWS Regions.
- D. Use databases that are hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Correct Answer: A

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling:EC2_INSTANCE_LAUNCH events.

Correct Answer: B

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes for an Amazon RDS table, and deletes -

the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Correct Answer: D

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```

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

```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Correct Answer: C

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

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

Correct Answer: A

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application. Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Correct Answer: *D*

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Correct Answer: *D*

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Correct Answer: *D*

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning functionality. This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon Elastic File System (Amazon EFS).
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon Elastic Block Store (Amazon EBS).

Correct Answer: *B*

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Correct Answer: *D*

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

Correct Answer: *B*

A company has an application that calls AWS Lambda functions. A code review shows that database credentials are stored in a Lambda function's source code, which violates the company's security policy. The credentials must be securely stored and must be automatically rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements in the MOST secure manner?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can use the key ID to retrieve the password from CloudHSM. Use CloudHSM to automatically rotate the password.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can use the secret ID to retrieve the password from Secrets Manager. Use Secrets Manager to automatically rotate the password.
- C. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can use the key ID to retrieve the password from AWS KMS. Use AWS KMS to automatically rotate the uploaded password.
- D. Move the database password to an environment variable that is associated with the Lambda function. Retrieve the password from the environment variable by invoking the function. Create a deployment script to automatically rotate the password.

Correct Answer: *B*

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Correct Answer: *A*

A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution's cost should be minimal.

Which storage solution meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: *D*

A company's operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.

Which solution would satisfy these requirements?

- A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.
- B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.
- C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
- D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

Correct Answer: *D*

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Correct Answer: *A*

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences. The application is successful with a rapid increase in the number of users every month. The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon

RDS for MySQL instance has triggered alarms related to resource exhaustion due to read requests.

What can a solutions architect recommend to prevent service Interruptions at the database layer with minimal changes to code?

- A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.
- B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

Correct Answer: *A*

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.

- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.

Which solution should a solutions architect recommend that is MOST highly available?

- A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
- B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
- C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
- D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Correct Answer: C

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.

What should a solutions architect recommend?

- A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.
- D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Correct Answer: A

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.

- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Correct Answer: *B*

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Correct Answer: *A*

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Correct Answer: *B*

A public-facing web application queries a database hosted on an Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.

What should a solutions architect recommend to the application team? (Choose two.)

- A. Cache query data in Amazon SQS
- B. Create a read replica to offload queries
- C. Migrate the database to Amazon Athena
- D. Implement Amazon DynamoDB Accelerator to cache data.
- E. Migrate the database to Amazon RDS

Correct Answer: *BE*

A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

- A. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range.
- B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
- C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
- D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Correct Answer: C

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on

Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability to shift traffic from resources in one region to another.

What should a solutions architect recommend?

- A. Configure an Amazon Route 53 latency routing policy.
- B. Configure an Amazon Route 53 geolocation routing policy.
- C. Configure an Amazon Route 53 geoproximity routing policy.
- D. Configure an Amazon Route 53 multivalue answer routing policy.

Correct Answer: C

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share.

Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.

What should a solutions architect recommend to meet these requirements?

- A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.
- B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.
- C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
- D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Correct Answer: D

An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.

Which solution is the MOST cost-effective?

- A. DEV with Spot Instances and PROD with On-Demand Instances

- B. DEV with On-Demand Instances and PROD with Spot Instances
- C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
- D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Correct Answer: C

A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each EC2 instance.
- B. Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.
- C. Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Correct Answer: A

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: C

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.

- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Correct Answer: C

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.

Which database implementations will meet these requirements? (Choose two.)

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon RDS for MySQL
- D. MySQL-compatible Amazon Aurora Multi-AZ
- E. Amazon RDS for SQL Server Standard Edition Multi-AZ

Correct Answer: DE

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Correct Answer: C

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

```
Policy1
{
    "version": "2012-10-17", "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam>List*",
                "kms>List*",
                "ec2:*",
                "ds:*",
                "logs:Get*",
                "logs:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

```
Policy2
{
```

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

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

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

Correct Answer: C

A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connections to it.

How can a solutions architect achieve this objective?

- A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
- B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
- C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
- D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

Correct Answer: *B*

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

Correct Answer: *A*

A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

- A. Use step scaling.
- B. Use simple scaling.
- C. Use lifecycle hooks.
- D. Use scheduled scaling.

Correct Answer: *D*

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns. Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
- C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
- D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Correct Answer: B

A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis.

What is the MOST cost-effective storage solution alternative to the current configuration?

- A. Configure a lifecycle policy to delete the objects after 30 days.
- B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
- C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Correct Answer: D

A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited time. What should a solutions architect do to securely meet these requirements?

- A. Enable public access on an Amazon S3 bucket.
- B. Generate a presigned URL to share with the users.
- C. Encrypt files using AWS KMS and provide keys to the users.
- D. Create and assign IAM roles that will grant GetObject permissions to the users.

Correct Answer: B

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an

NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing. Which solution will meet these requirements?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
- B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

Correct Answer: A

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon S3.

What should a solutions architect recommend to satisfy these requirements?

- A. Server-side encryption with customer-provided encryption keys
- B. Client-side encryption with Amazon S3 managed encryption keys
- C. Server-side encryption with keys stored in AWS Key Management Service (AWS KMS)
- D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Correct Answer: D

A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
- B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
- C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
- D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.
- E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

Correct Answer: AB

A company is investigating potential solutions that would collect, process, and store users' service usage data. The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure

Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.

Which solution should a solutions architect recommend?

- A. Use an Amazon Timestream database.
- B. Use an Amazon Neptune database in a Multi-AZ design.
- C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.
- D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS) Throughput Optimized HDD (st1) storage.

Correct Answer: C

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.

How should a solutions architect optimize high availability for the application?

- A. Use Lambda@Edge for CloudFront.
- B. Use Amazon S3 Transfer Acceleration for CloudFront.
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Correct Answer: A

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Correct Answer: D

A company currently stores symmetric encryption keys in a hardware security module (HSM). A solutions architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys.

Where should the key material be stored to meet these requirements?

- A. Amazon S3
- B. AWS Secrets Manager
- C. AWS Systems Manager Parameter store
- D. AWS Key Management Service (AWS KMS)

Correct Answer: D

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Correct Answer: *D*

A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance. Which solution should the solutions architect recommend?

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

Correct Answer: *B*

A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet.

How should a solutions architect configure access?

- A. Create a private hosted zone using Amazon Route 53.
- B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
- C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.
- D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Correct Answer: *B*

A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low latency.

Which architecture should a solutions architect recommend for this situation?

- A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.
- B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.

- C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
- D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

Correct Answer: *D*

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: *C*

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the keys to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service (AWS KMS) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Correct Answer: *D*

A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a

Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed.

Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency.

What should a solutions architect recommend as replacement database?

- A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
- B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.

- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
- D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Correct Answer: *D*

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.

How should a solutions architect meet these requirements?

- A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
- C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

Correct Answer: *C*

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environments and with AWS.

Which services meet the business requirements? (Choose two.)

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Correct Answer: *CE*

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.

Which solution will accomplish this?

- A. Spot Fleet
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

Correct Answer: A

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances. What should a solutions architect do to accomplish this?

- A. Configure a volume using Amazon Elastic File System (Amazon EFS). Mount the EFS volume to each Windows instance.
- B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.
- C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: C 

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.

What should a solutions architect do to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check.
- C. Create an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Correct Answer: C

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.

Which method should the solutions architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.

- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Correct Answer: A 

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However, the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group.
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica.
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Correct Answer: C

A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. The IAM policy must prevent function from performing any other actions on the Books table or any other.

Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        }  
    ]  
}
```

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"  
        }  
    ]  
}
```

C.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}

```

D.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        },
        {
            "Sid": "putUpdateDeleteOnBooks",
            "Effect": "Deny",
            "Action": "dynamodb:*,*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}

```

Correct Answer: A

A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs.

What should a solutions architect do to reduce costs?

- A. Configure Amazon CloudFront with the existing website as the origin.
- B. Move the website to Amazon EC2 with Amazon Elastic Block Store (Amazon EBS) volumes for storage.
- C. Use AWS Global Accelerator and specify the existing website as the endpoint.
- D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Correct Answer: A

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.

How should the company deploy this solution?

- A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
- B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
- D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Correct Answer: A

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible

I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of

storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

- A. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: A

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 buckets it uses to store data. Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage.

Which solution will lower costs without compromising the availability of objects?

- A. Use S3 ACLs.
- B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.
- C. Use S3 Intelligent-Tiering storage.
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket. The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.

Which combination of actions should solutions archived take to accomplish this? (Choose two.)

- A. Create a VPC endpoint for Amazon S3.
- B. Enable server access logging on the bucket.
- C. Apply a bucket policy to restrict access to the S3 endpoint.
- D. Add an S3 ACL to the bucket that has sensitive information.
- E. Restrict users using the IAM policy to use the specific bucket.

Correct Answer: AC

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.

How can a solutions architect make the system more responsive?

- A. Use Amazon SQS with AWS Lambda to generate reports.
- B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
- C. Update the client-side application code to increase its request timeout to 5 minutes.

- D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Correct Answer: A

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.

What should the solutions architect do to meet these requirements?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Correct Answer: D

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.

Which action will be MOST effective in accomplishing this?

- A. Replace the SQS queue with Amazon Kinesis Data Firehose.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
- D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Correct Answer: D

A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads.

The application is critical to the business and must be highly available.

Which solution will meet these requirements?

- A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.
- B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.
- C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.
- D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

Correct Answer: C

A solutions architect must design a solution for a persistent database that is being migrated from on-premises to AWS. The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.

Which solution effectively meets the database administrator's criteria?

- A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
- B. Create a Nitro-based Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
- C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
- D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Correct Answer: B

A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

- A. An Auto Scaling group with Spot Instance types.
- B. A placement group using a cluster placement strategy.
- C. A placement group using a partition placement strategy.
- D. An Auto Scaling group with On-Demand instance types.

Correct Answer: B

A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.

What should a solutions architect recommend to reduce internet latency?

- A. Set up AWS Global Accelerator and add endpoints.
- B. Set up AWS Direct Connect locations in multiple Regions.
- C. Set up an Amazon CloudFront distribution to access an application.
- D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Correct Answer: A

A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.

The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.

Which services satisfies these security requirements?

- A. AWS CloudHSM with the CloudHSM client

- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Correct Answer: A

A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.

Which solution meets these requirements?

- A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.
- D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

Correct Answer: A

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A

A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost-effective. Which combination of AWS services and features should the solutions architect use? (Choose two.)

- A. Amazon S3
- B. Amazon EC2

- C. AWS Fargate
- D. Amazon CloudFront
- E. Elastic Load Balancer

Correct Answer: AD

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Correct Answer: C

A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours.

Which solutions can accomplish this? (Choose two.)

- A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
- B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
- C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
- D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
- E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

Correct Answer: AB

A company has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-1 Region. A solutions architect is designing a disaster recovery strategy to have the database provisioned in the us-west-2 Region in case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

- A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.

- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
- D. Create a multimaster read/write instances across multiple AWS Regions. Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Correct Answer: *B*

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.

What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Correct Answer: *A*

A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center.

The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.

What should the solutions architect do to meet these requirements?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS)
- C. Set up AWS Storage Gateway as a volume gateway
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: *A*

A solutions architect is designing a hybrid application using the AWS cloud. The network between the on-premises data center and AWS will use an AWS Direct Connect (DX) connection. The application connectivity between AWS and the on-premises data center must be highly resilient.

Which DX configuration should be implemented to meet these requirements?

- A. Configure a DX connection with a VPN on top of it.
- B. Configure DX connections at multiple DX locations.

- C. Configure a DX connection using the most reliable DX partner.
- D. Configure multiple virtual interfaces on top of a DX connection.

Correct Answer: *B*

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.

Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

- A. Deploy a NAT instance in a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Correct Answer: *B*

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon

RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running.

The business reporting users must be able to generate reports without affecting the application's performance. Which action will accomplish this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Correct Answer: *D*

A company is running a two-tier ecommerce website using AWS services. The current architect uses a publish-facing Elastic Load Balancer that sends traffic to

Amazon EC2 instances in a private subnet. The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MySQL database. The application is running in the United States. The company recently started selling to users in Europe and Australia. A solutions architect needs to design solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances.
- D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Correct Answer: *B*

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective,

limit the provisioning of infrastructure resources, and provide the fastest possible response time. Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A

A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server databases running on Amazon EC2 instances with Windows Server 2016. The solution must be able to be integrated into the corporate Active Directory domain, be highly durable, be managed by AWS, and provide high levels of throughput and IOPS. Which solution meets these requirements?

- A. Use Amazon FSx for Windows File Server.
- B. Use Amazon Elastic File System (Amazon EFS).
- C. Use AWS Storage Gateway in file gateway mode.
- D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Correct Answer: A

A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions. The company wants to create an allow list for the IPs of all the load balancers on its firewall device. A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall.

What should the solutions architect recommend to meet these requirements?

- A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IPs. Register the private IPs of all the ALBs as targets to this NLB.
- C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.
- D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

Correct Answer: C

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.

- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: *B*

A company is planning to migrate its virtual server-based workloads to AWS. The company has internet-facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository.

Which services should a solutions architect recommend be hosted on the public subnet? (Choose two.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Correct Answer: *AC*

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Correct Answer: *B*

A company is using a tape backup solution to store its key application data offsite. The daily data volume is around 50 TB. The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed, and a week's notice is typically given if a backup needs to be restored.

The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes. The company also wants to make sure that the transition from tape backups to the cloud minimizes disruptions.

Which storage solution is MOST cost-effective?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

Correct Answer: A

A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead.

Which solution should the solutions architect implement?

- A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.
- B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
- C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
- D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Correct Answer: A

A company decides to migrate its three-tier web application from on-premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.

Which AWS service meets these requirements?

- A. Amazon Aurora
- B. Amazon RDS for SqlServer
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB on-demand

Correct Answer: A

A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.

Which method should a solutions architect implement to meet this requirement?

- A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs.
- B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs.
- C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs.
- D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

Correct Answer: D

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross-communication. A recent increase in account creations and

VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect

has been tasked with creating a centrally managed networking setup for multiple accounts, VPCs, and VPNs. Which networking solution meets these requirements?

- A. Configure shared VPCs and VPNs and share to each other.
- B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect connection between all VPCs and VPNs.
- D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

Correct Answer: *D*

A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.

Which database solution meets these requirements?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Correct Answer: *B*

A solutions architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file Share to Amazon RDS.
- B. Migrate the file Share to AWS Storage Gateway
- C. Migrate the file Share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Correct Answer: *C*

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Correct Answer: *A*

A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low. If an Availability Zone fails, how can the company remain compliant with the SLA?

- A. Add a target tracking scaling policy with a short cooldown period.
- B. Change the Auto Scaling group launch configuration to use a larger instance type.
- C. Change the Auto Scaling group to use six servers across three Availability Zones.
- D. Change the Auto Scaling group to use eight servers across two Availability Zones.

Correct Answer: A 

A company is reviewing its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization. A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

- A. Enable AWS Config service with the appropriate rules
- B. Enable AWS Trusted Advisor with the appropriate checks.
- C. Write a script using an AWS SDK to generate a bucket report
- D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Correct Answer: A

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency.

What should a solutions architect recommend to meet these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.
- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Correct Answer: B

A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain.

Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).

- B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

Correct Answer: *D*

A solutions architect has configured the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "lambda:CreateFunction",
        "lambda>DeleteFunction"
      ],
      "Resource": "*"
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "220.100.16.0/20"
        }
      }
    }
  ]
}
```

Which action will be allowed by the policy?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

Correct Answer: *C*

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an

Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files. Which storage option meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: *B*

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

- A. Move static assets to Amazon CloudFront. Leave the application in EC2 in an Auto Scaling group. Move the database to Amazon RDS to deploy Multi-AZ.
- B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.
- C. Move static assets to Amazon S3. Move the application to AWS Lambda with the concurrency limit set. Move the database to Amazon DynamoDB with on-demand enabled.
- D. Move static assets to Amazon S3. Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled. Move the database to Amazon RDS to deploy Multi-AZ.

Correct Answer: *A* 

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content. This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

- A. Change the EBS volume to Provisioned IOPS (PIOPS).
- B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.
- C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.
- D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Correct Answer: *B*

A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files

while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

- A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.
- B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
- D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
- E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Correct Answer: AC

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists. The company is looking for a native, software-based AWS service to accomplish this goal.

What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Correct Answer: A

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

Correct Answer: C

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Correct Answer: *B*

A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.

Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Choose two.)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Correct Answer: *CD*

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only.

What should a solutions architect do to protect against data loss? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Correct Answer: *AE*

An operations team has a standard that states IAM policies should not be applied directly to users. Some new team members have not been following this standard. The operations manager needs a way to easily identify the users with attached policies.

What should a solutions architect do to accomplish this?

- A. Monitor using AWS CloudTrail.
- B. Create an AWS Config rule to run daily.
- C. Publish IAM user changes to Amazon SNS.

- D. Run AWS Lambda when a user is modified.

Correct Answer: C

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.

Which solution should the solutions architect select?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Correct Answer: C

A company is building applications in containers. The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS. Management states that production systems must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software.

Which solution meets these requirements?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS worker nodes.
- C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

Correct Answer: B

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling. Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy.

Correct Answer: D

A solutions architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load

Balancer. The solutions architect must improve the security posture and minimize the impact of a DDoS attack on resources.

Which solution is MOST effective?

- A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.
- B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
- C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
- D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

Correct Answer: *B*

A company has multiple AWS accounts for various departments. One of the departments wants to share an Amazon S3 bucket with all other departments.

Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket.
- B. Create a pre-signed URL for the bucket and share it with other departments.
- C. Set the S3 bucket policy to allow cross-account access to other departments.
- D. Create IAM users for each of the departments and configure a read-only IAM policy.

Correct Answer: *C*

A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.

Which action should be taken to share the S3 bucket?

- A. Update the bucket to be a Requester Pays bucket.
- B. Update the bucket to enable cross-origin resource sharing (CORS).
- C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.
- D. Create an IAM policy to require users to grant bucket-owner-full-control when uploading objects.

Correct Answer: *C* 

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Correct Answer: *B*

A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.

What is the FASTEST way to aggregate data from all of these global sites?

- A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
- B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

Correct Answer: *A*

A company has a custom application running on an Amazon EC instance that:

- * Reads a large amount of data from Amazon S3
- * Performs a multi-stage analysis
- * Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis. The process performance depends on the temporary storage performance.

What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.
- B. Multiple Amazon Elastic Block Store (Amazon EBS) drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon Elastic File System (Amazon EFS) volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Correct Answer: *A*

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when

the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Correct Answer: *B*

A company recently released a new type of internet-connected sensor. The company is expecting to sell thousands of sensors, which are designed to stream high volumes of data each second to a central location. A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness.

Which solution should the solutions architect recommend?

- A. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- B. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
- C. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Correct Answer: *D*

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.

How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Correct Answer: *C*

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available fault

tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Correct Answer: C

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing.

Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Correct Answer: B 

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

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

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Correct Answer: AE

A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for a minimum of two instances and a

maximum of four instances across two Availability Zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for all the EC2 instances.

What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

- A. Remove some EC2 instances to increase the utilization of remaining instances.
- B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
- C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
- D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

Correct Answer: *D*

A company has an application that posts messages to Amazon SQS. Another application polls the queue and processes the messages in an I/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages, the company has difficulty meeting its SLA consistently. What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

- A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.
- B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance.
- C. Create an Amazon Machine image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy to keep its aggregate CPU utilization below 70%.
- D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

Correct Answer: *D*

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls. What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Correct Answer: A

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

Correct Answer: B

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to further reduce data transfer costs. The company cannot modify the application's source code.

What should a solutions architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Correct Answer: A

A database is on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that experiences highly dynamic reads. Application developers notice a significant slowdown when testing read performance from a secondary AWS Region. The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

- A. Install MySQL on Amazon EC2 in the secondary Region.
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary Region.
- D. Implement Amazon ElastiCache to improve database query performance.

Correct Answer: B

A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days.

Which solution should a solutions architect recommend?

- A. Set the backup retention period to 90 days when creating the RDS DB instance.
- B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.
- C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days. Create an AWS Backup job to schedule the execution of the backup plan daily.
- D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot. Purge snapshots older than 90 days.

Correct Answer: B

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation.

What should a solutions architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.
- D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Correct Answer: D

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority. Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Correct Answer: A

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various

storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS Amazon Elastic File System (Amazon EFS) storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Correct Answer: *D*

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: *C*

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure. The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Correct Answer: *B*

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

- A. Place all the EC2 instances in an Auto Scaling group.
- B. Place all the EC2 instances in the same AWS Region.
- C. Place all the EC2 instances in the same Availability Zone.

- D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Correct Answer: C

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

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

Correct Answer: D

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Correct Answer: B

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.

What should the solutions architect recommend to build the MOST high-performing solution?

- A. Use AWS Glue to process data and Amazon S3 to store data.
- B. Use Amazon EMR to process data and Amazon Redshift to store data.
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

Correct Answer: B

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

- A. Launch an Amazon ElastiCache cluster to cache common database queries.
- B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
- C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.
- D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

Correct Answer: *B*

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends. A solutions architect needs to design a cost-effective solution that can handle the load. What should the solutions architect do to meet these requirements?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable Multi-AZ replication for the DynamoDB database.
- C. Enable DynamoDB auto scaling when creating the tables.
- D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Correct Answer: *C*

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

- A. Enable concurrency scaling.
- B. Enable cross-Region snapshots.
- C. Increase the data retention period.
- D. Deploy Amazon Redshift in Multi-AZ.

Correct Answer: *B*

A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

- A. Amazon Redshift
- B. AWS Storage Gateway for files
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Correct Answer: B

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF. How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Correct Answer: D

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company's needs and takes the LEAST amount of time?

- A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.
- B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.
- C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.
- D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

Correct Answer: D

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Correct Answer: A

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.

What should a solutions architect recommend?

- A. Set up a new Direct Connect connection in another AWS Region.
- B. Set up a new AWS managed VPN connection in another AWS Region.
- C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
- D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

Correct Answer: C

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

Correct Answer: A

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B

A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short

Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.

What should a solutions architect recommend?

- A. Use Amazon DynamoDB global tables.
- B. Use Amazon Aurora Global Database.
- C. Use Amazon RDS for MySQL with a cross-Region read replica.
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

Correct Answer: A

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Correct Answer: AE

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.

Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

- A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
- B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
- C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
- D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

Correct Answer: A

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored. The amount of data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived

and deleted, the storage size is not expected to exceed 1 TB.

Which storage solution should the solutions architect recommend?

- A. An Amazon DynamoDB table accessible by all ECS cluster instances.
- B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
- C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
- D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

Correct Answer: C

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.

Which configuration should a solutions architect recommend?

- A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.
- B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.
- C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
- D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

Correct Answer: A

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B

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

Which storage solution meets these requirements?

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering

- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: *B*

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

- A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
- D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

Correct Answer: *A*

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Correct Answer: *B*

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Correct Answer: *D*

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly. What is the MOST cost-effective method to establish this type of connection?

- A. Implement a client VPN.
- B. Implement AWS Direct Connect.
- C. Implement a bastion host on Amazon EC2.
- D. Implement an AWS Site-to-Site VPN connection.

Correct Answer: *D*

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year.

The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

- A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
- B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
- C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
- D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

Correct Answer: *C*

A company runs a high performance computing (HPC) workload on AWS. The workload required low-latency network performance and high network throughput with tightly coupled node-to-node communication. The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.

What should a solutions architect propose to improve the performance of the workload?

- A. Choose a cluster placement group while launching Amazon EC2 instances.
- B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
- C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
- D. Choose the required capacity reservation while launching Amazon EC2 instances.

Correct Answer: A

A company uses a legacy on-premises analytics application that operates on gigabytes of .csv files and represents months of data. The legacy application cannot handle the growing size of .csv files. New .csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services. To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3. Which solution should the solutions architect recommend?

- A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company's on-premises storage and the company's S3 bucket.
- B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.
- C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.
- D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon Elastic File System (Amazon EFS) to the company's S3 bucket.

Correct Answer: B

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit. What should a solutions architect recommend?

- A. Set up a corporate Amazon S3 bucket and move all media and application files.
- B. Configure Amazon FSx for Windows File Server and move all the media and application files.
- C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
- D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

Correct Answer: B

A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances. What should a solutions architect do to ensure these requirements are met?

- A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.

- C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

Correct Answer: C

A company is experiencing growth as demand for its product has increased. The company's existing purchasing application is slow when traffic spikes. The application is a monolithic three-tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier. A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes. Which solution will meet these requirements?

- A. Vertically scale the application instance using a larger Amazon EC2 instance size.
- B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS.
- C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.
- D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

Correct Answer: C

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Correct Answer: B

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use of AWS Snowball.

What should a solutions architect recommend to accomplish this?

- A. Order a Snowball Edge device to copy the data from one Region to another Region.
- B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
- C. Use the aws s3 sync command to copy data from the source bucket to the destination bucket.
- D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

Correct Answer: D

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Correct Answer: A

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.

What should a solutions architect recommend?

- A. Use an Auto Scaling group with a cluster placement group.
- B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
- C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
- D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

Correct Answer: A

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Correct Answer: D

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.

What should a solutions architect recommend?

- A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
- B. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.
- C. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
- D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

Correct Answer: B

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3>ListBucket",
                "s3>DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

A.

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

B.

```
"Action": [
    "s3:*"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
C.
>Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"
D.
>Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

Correct Answer: A

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.

Correct Answer: C

A company wants to share forensic accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and requires its own copy of the database. How should the company securely share the database with the auditor?

- A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.
- B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.
- C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.
- D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

Correct Answer: A

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

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

Correct Answer: A

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.

The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.

- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Correct Answer: C

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Correct Answer: B

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

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

Correct Answer: B

A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access. The application will use Amazon

EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the

Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost?

- A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.
- B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.

- C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.
- D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

Correct Answer: *D*

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBC snapshots are encrypted.

What should the solutions architect do to accomplish this?

- A. Enable EBS encryption by default for the AWS Region.
- B. Enable EBS encryption by default for the specific volumes.
- C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.
- D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

Correct Answer: *C*

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.

What should a solutions architect recommend to meet these requirements?

- A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
- B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
- C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
- D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Correct Answer: *D*

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

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

Correct Answer: *A*

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce costs.

What should a solutions architect recommend?

- A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.
- B. Implement CloudFront events with Lambda@Edge to run the website's data processing.
- C. Modify the CloudFront price class to include only the locations of the countries that are served.
- D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

Correct Answer: C

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year. Which Amazon EC2 pricing option is the MOST cost-effective?

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

Correct Answer: A

A company is designing a website that uses an Amazon S3 bucket to store static images. The company wants all future requests to have faster response times while reducing both latency and cost.

Which service configuration should a solutions architect recommend?

- A. Deploy a NAT server in front of Amazon S3.
- B. Deploy Amazon CloudFront in front of Amazon S3.
- C. Deploy a Network Load Balancer in front of Amazon S3.
- D. Configure Auto Scaling to automatically adjust the capacity of the website.

Correct Answer: B

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

Correct Answer: A

A company needs to comply with a regulatory requirement that states all emails must be stored and archived externally for 7 years. An administrator has created compressed email files on premises and wants a managed

service to transfer the files to AWS storage.

Which managed service should a solutions architect recommend?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon S3 Glacier
- C. AWS Backup
- D. AWS Storage Gateway

Correct Answer: D

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named CompanyConfidential. The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.

Which IAM policy will meet these requirements?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListBucket",
            "Resource": "arn:aws:s3:::AdminTools"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
```

C.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*",
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}

```

D.

```

"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": "s3>ListBucket",
        "Resource": "arn:aws:s3:::AdminTools/*"
    },
    {
        "Effect": "Allow",
        "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],
        "Resource": "arn:aws:s3:::AdminTools/*"
    },
    {
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::CompanyConfidential",
            "arn:aws:s3:::CompanyConfidential/*",
            "arn:aws:s3:::AdminTools/*"
        ]
    }
]

```

Correct Answer: C

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.

What should a solutions architect do to accomplish this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Correct Answer: A

A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS.

Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.

The company wants a highly scalable solution with no server maintenance nor advanced capacity planning. Which solution meets these requirements?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
- B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

Correct Answer: *B*

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Choose two.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53.
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Correct Answer: *BE*

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.

What should a solutions architect do to minimize the anticipated server load?

- A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.
- B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
- C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
- D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

Correct Answer: *C*

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime. Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Correct Answer: C

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solutions architect recommend to provide a highly available and scalable solution?

- A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
- B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
- C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.
- D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

Correct Answer: A

Management has decided to deploy all AWS VPCs with IPv6 enabled. After some time, a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet.

What should the solutions architect do to fix this?

- A. Check to make sure that only IPv6 was used during the VPC creation.
- B. Create a new IPv4 subnet with a larger range, and then launch the instance.
- C. Create a new IPv6-only subnet with a large range, and then launch the instance.
- D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

Correct Answer: C

A company has a build server that is in an Auto Scaling group and often has multiple Linux instances running. The build server requires consistent and mountable shared NFS storage for jobs and configurations.

Which storage option should a solutions architect recommend?

- A. Amazon S3
- B. Amazon FSx

- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Correct Answer: D

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a

NAT instance for internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

- A. Configure a NAT gateway to replace the NAT instances.
- B. Configure a gateway endpoint for traffic destined to Amazon S3.
- C. Configure an interface endpoint for traffic destined to Amazon S3.
- D. Configure Amazon CloudFront for the S3 bucket storing the images.

Correct Answer: C

The financial application at a company stores monthly reports in an Amazon S3 bucket. The vice president of finance has mandated that all access to these reports be logged and that any modifications to the log files be detected.

Which actions can a solutions architect take to meet these requirements?

- A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled.
- B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled.
- C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.
- D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

Correct Answer: C

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.

- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Correct Answer: D

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company's account. All the needed policies have been created to grant appropriate access.

Which additional component will provide the vendor with the MOST secure access to the account?

- A. Create an IAM user.
- B. Implement a service control policy (SCP)
- C. Use a cross-account role with an external ID.
- D. Configure a single sign-on (SSO) identity provider.

Correct Answer: B

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Correct Answer: AD

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS.

However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.
- C. Build a database cache using Amazon ElastiCache.
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Correct Answer: A

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices.

The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.
- B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

Correct Answer: A

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users. During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Correct Answer: C

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Correct Answer: C

A company is backing up on-premises databases to local file server shares using the SMB protocol. The company requires immediate access to 1 week of backup files to meet recovery objectives. Recovery after a week is less likely to occur, and the company can tolerate a delay in accessing those older backup files. What should a solutions architect do to meet these requirements with the LEAST operational effort?

- A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.
- B. Deploy an AWS Storage Gateway file gateway with sufficient storage to hold 1 week of backups. Point the backups to SMB shares from the file gateway.
- C. Deploy Amazon Elastic File System (Amazon EFS) to create a file system with exposed NFS shares with sufficient storage to hold all the desired backups.
- D. Continue to back up to the existing file shares. Deploy AWS Database Migration Service (AWS DMS) and define a copy task to copy backup files older than 1 week to Amazon S3, and delete the backup files from the local file store.

Correct Answer: A

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon

EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a period of time during surges. A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

Correct Answer: D

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solutions architect needs to bring that data on premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.

- D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Correct Answer: B

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution. What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Correct Answer: A

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

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

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

Correct Answer: B

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be executed when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be executed when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Correct Answer: *D*

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Correct Answer: *B*

A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled. For compliance reasons, the older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.

What should the solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use S3 batch operations to replace object tags. Expire the objects based on the modified tags.
- B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.
- C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SQS) queue for further processing.
- D. Replicate older object versions to a new bucket. Use an S3 Lifecycle policy to expire the objects in the new bucket after 2 years.

Correct Answer: *B*

A company runs an application on an Amazon EC2 instance backed by Amazon Elastic Block Store (Amazon EBS). The instance needs to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application. However, the contents of the instance's memory must be preserved whenever the instance is unavailable.

What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
- D. Terminate the instance outside the application's availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Correct Answer: *B*

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Correct Answer: C

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by a way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Correct Answer: B

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

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

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

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Correct Answer: *B*

A company is moving its on-premises applications to Amazon EC2 instances. However, as a result of fluctuating compute requirements, the EC2 instances must always be ready to use between 8 AM and 5 PM in specific Availability Zones.

Which EC2 instances should the company choose to run the applications?

- A. Scheduled Reserved Instances
- B. On-Demand Instances
- C. Spot Instances as part of a Spot Fleet
- D. EC2 instances in an Auto Scaling group

Correct Answer: *A*

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Correct Answer: *D*

A company is building an application on Amazon EC2 instances that generates temporary transactional data. The application requires access to data storage that can provide configurable and consistent IOPS.

What should a solutions architect recommend?

- A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
- B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
- C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.
- D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

Correct Answer: C

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.

Which storage solution meets these requirements?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Correct Answer: B

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Correct Answer: D

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting high request latency for users located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

How should a solutions architect accomplish this?

- A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
- C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Correct Answer: *B*

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users. The service is hosted in a VPC behind a

Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.

What should a solutions architect do to accomplish this goal?

- A. Create a peering VPC connection from each user's VPC to the software vendor's VPC.
- B. Deploy a transit VPC in the software vendor's AWS account. Create a VPN connection with each user account.
- C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.
- D. Deploy a transit VPC in the software vendor's AWS account. Create an AWS Direct Connect connection with each user account.

Correct Answer: *C*

A user wants to list the IAM role that is attached to their Amazon EC2 instance. The user has login access to the EC2 instance but does not have IAM permissions.

What should a solutions architect do to retrieve this information?

- A. Run the following EC2 command: curl <http://169.254.169.254/latest/meta-data/iam/info>
- B. Run the following EC2 command: curl <http://169.254.169.254/latest/user-data/iam/info>
- C. Run the following EC2 command: <http://169.254.169.254/latest/dynamic/instance-identity/>
- D. Run the following AWS CLI command: aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

Correct Answer: A

A company has an application that is hosted on Amazon EC2 instances in two private subnets. A solutions architect must make the application available on the public internet with the least amount of administrative effort. What should the solutions architect recommend?

- A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.
- D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two private subnets from the same Availability Zones as the public instances.

Correct Answer: C

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Correct Answer: C

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

Correct Answer: A

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

What should the solutions architect do to meet this requirement?

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

Correct Answer: B

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL. In the database layer several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Correct Answer: D

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: B

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

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

Correct Answer: D

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.

The following are the key requirements:

- ☞ The web servers must be accessible only to users on an SSL connection.

☞ The database should be accessible to the web layer, which is created in a public subnet only.

☞ All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Choose two.)

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0).
- B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
- C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.
- E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Correct Answer: BD

A company has an on-premises application that collects data and stores it to an on-premises NFS server. The company recently set up a 10 Gbps AWS Direct

Connect connection. The company is running out of storage capacity on premises. The company needs to migrate the application data from on premises to the

AWS Cloud while maintaining low-latency access to the data from the on-premises application.

What should a solutions architect do to meet these requirements?

- A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.
- C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

Correct Answer: A

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement and support the NFS protocol.

Which solution meets these requirements?

- A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
- B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the instances and apply that to the additional instance.

- C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 instances that need access to the data.
- D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Correct Answer: A

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability. The company wants to be able to deploy updates to its application even if nodes in one Availability Zone are not accessible.

The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to 100%.

Which configuration of tasks and Availability Zones meets these requirements?

- A. Deploy the application across two Availability Zones, with one task in each Availability Zone.
- B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
- C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
- D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

Correct Answer: A

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Correct Answer: A

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

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

- D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.
- E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints

Correct Answer: AD

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application

Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed. What should the solutions architect do to ensure that the architecture supports distributed session data management?

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

Correct Answer: A

A company has an ecommerce application running in a single VPC. The application stack has a single web server and an Amazon RDS Multi-AZ DB instance.

The company launches new products twice a month. This increases website traffic by approximately 400% for a minimum of 72 hours. During product launches, users experience slow response times and frequent timeout errors in their browsers.

What should a solutions architect do to mitigate the slow response times and timeout errors while minimizing operational overhead?

- A. Increase the instance size of the web server.
- B. Add an Application Load Balancer and an additional web server.
- C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.
- D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

Correct Answer: A

A solutions architect is designing an architecture to run a third-party database server. The database software is memory intensive and has a CPU-based licensing model where the cost increases with the number of vCPU cores within the operating system. The solutions architect must select an Amazon EC2 instance with sufficient memory to run the database software, but the selected instance has a large number of vCPUs. The solutions architect must ensure that the vCPUs will not be underutilized and must minimize costs.

Which solution meets these requirements?

- A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.

- B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.
- C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.
- D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

Correct Answer: A

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: D

A company is creating a web application that will store a large number of images in Amazon S3. The images will be accessed by users over variable periods of time. The company wants to:

- Retain all the images
- Incur no cost for retrieval.
- Have minimal management overhead.
- Have the images available with no impact on retrieval time.

Which solution meets these requirements?

- A. Implement S3 Intelligent-Tiering
- B. Implement S3 storage class analysis
- C. Implement an S3 Lifecycle policy to move data to S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Implement an S3 Lifecycle policy to move data to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.

- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Correct Answer: C

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order, two microservices should handle the event simultaneously. The Email microservice will send a confirmation email, and the OrderProcessing microservice will start the order delivery process. If a customer cancels an order, the OrderCancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

- A. Create a single SQS queue and publish order events to it. The Email, OrderProcessing, and OrderCancellation microservices can then consume messages off the queue.
- B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email, OrderProcessing, and OrderCancellation microservices to its own topic.
- C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email, OrderProcessing, and OrderCancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.
- D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and OrderCancellation microservices.

Correct Answer: D

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL

Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon Elastic Block Store (Amazon EBS)

General Purpose SSD (gp2) volume. The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6.000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a Magnetic volume.
- B. Increase the number of IOPS on the gp2 volume.
- C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
- D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Correct Answer: C

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is

shared across a cluster of Linux servers. The company wants to reduce storage costs for the application. What should a solutions architect do to meet these requirements?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon Elastic File System (Amazon EFS) and store them locally on each Amazon EC2 instance.
- C. Configure a Lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
- D. Move the files to Amazon S3 with S3 lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

Correct Answer: C

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

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

Correct Answer: D

A company wants to migrate its web application to AWS. The legacy web application consists of a web tier, an application tier, and a MySQL database. The re-architected application must consist of technologies that do not require the administration team to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Choose two.)

- A. Amazon Aurora Serverless

- B. Amazon EC2 Spot Instances
- C. Amazon Elasticsearch Service (Amazon ES)
- D. Amazon RDS for MySQL
- E. AWS Fargate

Correct Answer: DE

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier two application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Correct Answer: B

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.
- D. Increase the Provisioned IOPS on the Aurora instance.

Correct Answer: D

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic Fife System (Amazon EFS) volumes and mount them to on-premises servers.

Correct Answer: DE

A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Amazon EC2 instances in private subnets Configure. Configure a public Application Load Balancer with multiple redundant Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Correct Answer: B

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in- memory cache for DynamoDB hosting the application data.

Correct Answer: D

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in

Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

- A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group

- for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
 - C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
 - D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Correct Answer: C

A development team stores its Amazon RDS MySQL DB instance user name and password credentials in a configuration file. The configuration file is stored as plaintext on the root device volume of the team's Amazon EC2 instance. When the team's application needs to reach the database, it reads the file and loads the credentials into the code. The team has modified the permissions of the configuration file so that only the application can read its content. A solutions architect must design a more secure solution.

What should the solutions architect do to meet this requirement?

- A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.
- B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.
- C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.
- D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

Correct Answer: D

A company wants a storage option that enables its data science team to analyze its data on premises and in the AWS Cloud. The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones.

What should a solutions architect do to meet these requirements?

- A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
- B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
- C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

Correct Answer: C

A company wants to improve the availability and performance of its stateless UDP-based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions.

What should a solutions architect recommend to accomplish this?

- A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
- B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.
- C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
- D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

Correct Answer: D

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling.

The company's HPC workloads run on Linux. Each

HPC workflow runs on hundreds of AmazonEC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead from aging and scaling the database must be minimized.

Which database solution should the solutions architect recommend?

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

Correct Answer: A

A company is working with an external vendor that requires write access to the company's Amazon Simple Queue Service (Amazon SQS) queue. The vendor has its own AWS account.

What should a solutions architect do to implement least privilege access?

- A. Update the permission policy on the SQS queue to give write access to the vendor's AWS account.
- B. Create an IAM user with write access to the SQS queue and share the credentials for the IAM user.
- C. Update AWS Resource Access Manager to provide write access to the SQS queue from the vendor's AWS account.
- D. Create a cross-account role with access to all SQS queues and use the vendor's AWS account in the trust document for the role.

Correct Answer: D

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.

The tracking will need to read as fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of packages might be tracked on other days. Tracking will need to be searchable by tracking ID, customer ID, and order ID. Older than 1 month no longer need to be tracked.

What should a solutions architect recommend to accomplish this with minimal cost of ownership?

- A. Use Amazon DynamoDB with Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
- B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.
- C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
- D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.

Correct Answer: B

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

Correct Answer: C

A company needs to store data in Amazon S3. A compliance requirement states that when any changes are made to objects the previous state of the object with any changes must be preserved. Additionally, files older than 5 years should not be accessed but need to be archived for auditing.

What should a solutions architect recommend that is MOST cost-effective?

- A. Enable object-level versioning and S3 Object Lock in governance mode
- B. Enable object-level versioning and S3 Object Lock in compliance mode
- C. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive
- D. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: C

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Correct Answer: DE

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings in the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur they will happen very quickly.

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary Index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this

new service to affect the performance of the current application.

What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Correct Answer: A

A company is preparing to deploy a new serverless workload. A solutions architect needs to configure permissions for invoking an AWS Lambda function. The function will be triggered by an Amazon EventBridge (Amazon CloudWatch Events) rule. Permissions should be configured using the principle of least privilege. Which solution will meet these requirements?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:'* as the action and Service:events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Correct Answer: C

A company is building its web application using containers on AWS. The company requires three instances of the web application to run at all times. The application must be able to scale to meet increases in demand.

Management is extremely sensitive to cost but agrees that the application should be highly available.

What should a solutions architect recommend?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

Correct Answer: D

A company is Re-architecting a strongly coupled application to be loosely coupled. Previously the application used a request/response pattern to communicate between tiers. The company plans to use Amazon Simple Queue Service (Amazon SQS) to achieve decoupling requirements. The initial design contains one queue for requests and one for responses. However, this approach is not processing all the messages as the application scales. What should a solutions architect do to resolve this issue?

- A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.
- B. Configure a FIFO queue, and use the message deduplication ID and message group ID.
- C. Create a temporary queue, with the Temporary Queue Client to receive each response message.
- D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

Correct Answer: A

A company is launching an ecommerce website on AWS. This website is built with a three-tier architecture that includes a MySQL database in a Multi-AZ deployment of Amazon Aurora MySQL. The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones. The application produces a metric that describes the load the application experiences. Which solution meets these requirements?

- A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling.
- B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
- C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.
- D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

Correct Answer: B

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

Correct Answer: A

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B.

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

- A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Correct Answer: B

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3. Which solution meets these requirements and is MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Correct Answer: C

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

Which solution meets these requirements?

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

Correct Answer: B

A company has multiple applications that use Amazon RDS for MySQL as its database. The company recently discovered that a new custom reporting application has increased the number of Queries on the database. This is

slowing down performance.

How should a solutions architect resolve this issue with the LEAST amount of application changes?

- A. Add a secondary DB instance using Multi-AZ.
- B. Set up a read replica and Multi-AZ on Amazon RDS.
- C. Set up a standby replica and Multi-AZ on Amazon RDS.
- D. Use caching on Amazon RDS to improve the overall performance.

Correct Answer: D

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that security and compliance standards are being followed throughout the development process.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.
- B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.
- C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

Correct Answer: C

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month. Which analytics strategy is MOST cost-effective for the company to use?

- A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.
- B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.
- C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.
- D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

Correct Answer: A

A company wants to move its on-premises network attached storage (NAS) to AWS. The company wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time.

Which solution meets these requirements and is MOST cost-effective?

- A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.

- B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.
- C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.
- D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

Correct Answer: D

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.

How should the company write its application to handle these database requests?

- A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
- B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Correct Answer: A

A company that recently started using AWS establishes a Site-to-Site VPN between its on-premises datacenter and AWS. The company's security mandate states that traffic originating from on premises should stay within the company's private IP space when communicating with an Amazon Elastic Container Service (Amazon ECS) cluster that is hosting a sample web application.

Which solution meets this requirement?

- A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.
- B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.
- C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.
- D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

Correct Answer: C

A solutions architect must analyze and update a company's existing IAM policies prior to deploying a new workload. The solutions architect created the following policy:

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "NotAction": "s3:PutObject",
            "Resource": "*",
            "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}
        }
    ]
}
```

What is the net effect of this policy?

- A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.
- C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

Correct Answer: D

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a

PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: CD

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D

A company is using Amazon DynamoDB with provisioned throughput for the database tier of its ecommerce website. During flash sales, customers experience periods of time when the database cannot handle the high number of transactions taking place. This causes the company to lose transactions. During normal periods, the database performs appropriately.

Which solution solves the performance problem the company faces?

- A. Switch DynamoDB to on-demand mode during flash sales.
- B. Implement DynamoDB Accelerator for fast in memory performance.
- C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.
- D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

Correct Answer: A 

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B

A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.

What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

- A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
- B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

Correct Answer: B

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so. How should a solutions architect provide access to the SQS queue?

- A. Create an instance profile that provides the other company access to the SQS queue.
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Correct Answer: C

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and a paid tier. Users in the paid tier will have their videos converted first, and then the free tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

- A. One FIFO queue for the paid tier and one standard queue for the free tier.
- B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

Correct Answer: D

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts.

Which AWS service can the administrator use to protect the company against attacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

Correct Answer: C

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances. What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table.
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Correct Answer: D

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon

Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon Elastic File System (Amazon EFS) for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

Correct Answer: A

A company wants to host its web application on AWS using multiple Amazon EC2 instances across different AWS Regions. Since the application content will be specific to each geographic region, the client requests need to be routed to the server that hosts the content for that clients Region.

What should a solutions architect do to accomplish this?

- A. Configure Amazon Route 53 with a latency routing policy.
- B. Configure Amazon Route 53 with a weighted routing policy.
- C. Configure Amazon Route 53 with a geolocation routing policy.
- D. Configure Amazon Route 53 with a multivalue answer routing policy

Correct Answer: C

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability. Which solution meets these requirements?

- A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
- B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
- C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
- D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Correct Answer: A

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new

features every month. The startup team needs to minimize operational overhead costs. What should a solutions architect recommend to accomplish this?

- A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
- B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
- C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.
- D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

Correct Answer: C

A company is building a payment application that must be highly available even during regional service disruptions. A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions. The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports. The development team also needs to use SQL.

Which data storage solution meets these requirements?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon S3 with cross-Region replication and Amazon Athena
- D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

Correct Answer: C

A company stores call recordings on a monthly basis. Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year.

Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost.

Which solution is MOST cost-effective?

- A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier. Query S3 Glacier tags and retrieve the files from S3 Glacier.
- B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
- C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

Correct Answer: B

A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

- A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.
- B. The requests from the API are sent to the models' Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events. AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.
- C. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.
- D. The requests from the API are sent to the models' Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

Correct Answer: D

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

- A. Amazon S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

Correct Answer: D

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an

Elastic Load Balancer (ELB). A third party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

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

Correct Answer: C

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: D

A company is running a multi-tier web application on AWS. The application runs its database tier on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region. A database administrator who regularly monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPUUtilization on the read replica and causing increased read latency of the application.

What should a solutions architect do to improve read scalability?

- A. Reboot the Aurora DB cluster.
- B. Create a cross-Region read replica
- C. Increase the instance class of the read replica.
- D. Configure Aurora Auto Scaling for the read replica.

Correct Answer: D

A company's order fulfillment service uses a MySQL database. The database needs to support a large number of concurrent queries and transactions. Developers are spending time patching and tuning the database. This is causing delays in releasing new product features.

The company wants to use cloud-based services to help address this new challenge. The solution must allow the developers to migrate the database with little or no code changes and must optimize performance.

Which service should a solutions architect use to meet these requirements?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon ElastiCache

- D. MySQL on Amazon EC2

Correct Answer: A

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company want to run complex transformation before transferring the data.

Which AWS service should a solutions architect recommend for this migration?

- A. AWS Snowball
- B. AWS Snowmobile
- C. AWS Snowball Edge Storage Optimize
- D. AWS Snowball Edge Compute Optimize

Correct Answer: D

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Correct Answer: A

A company is selling up an application to use an Amazon RDS MySQL DB instance. The database must be architected for high availability across Availability Zones and AWS Regions with minimal downtime.

How should a solutions architect meet this requirement?

- A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.
- B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.
- C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.
- D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

Correct Answer: B

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multi-value routing policy
- D. Geolocation routing policy

Correct Answer: C

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

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

Correct Answer: A

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states:

- ☞ Keys must be rotated every 90 days.
- ☞ Strict separation of duties between key users and key administrators must be implemented.
- ☞ Auditing key usage must be possible.

What should the solutions architect recommend?

- A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
- C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
- D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

Correct Answer: A

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

30 days.

Which storage solution is MOST cost-effective?

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

Correct Answer: C

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in the same Region.

Correct Answer: A

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in older.

What should a solutions architect recommend to decouple the system?

- A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.
- B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.
- D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

Correct Answer: C

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without

compromising security or redundancy.

Which solution meets these requirements?

- A. Replace the NAT gateway with a NAT instance.
- B. Replace the NAT gateway with an internet gateway.
- C. Replace the NAT gateway with a gateway VPC endpoint.
- D. Replace the NAT gateway with an AWS Direct Connect connection.

Correct Answer: C

A company hosts a website on premises and wants to migrate it to the AWS Cloud. The website exposes a single hostname to the internet but it routes its functions to different on-premises server groups based on the path of the URL. The server groups are scaled independently depending on the needs of the functions they support. The company has an AWS Direct Connect connection configured to its on-premises network.

What should a solutions architect do to provide path-based routing to send the traffic to the correct group of servers?

- A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.
- B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.
- C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.
- D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer for the group of servers supporting that path.

Correct Answer: B

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage auto scaling in RDS.
- B. Increase the RDS database instance size.
- C. Change the RDS database instance storage type to Provisioned IOPS.
- D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

Correct Answer: A

An ecommerce website is deploying its web application as Amazon Elastic Container Service (Amazon ECS) container instances behind an Application Load

Balancer (ALB). During periods of high activity, the website slows down and availability is reduced. A solutions architect uses Amazon CloudWatch alarms to receive notifications whenever there is an availability issue so they can scale out resources. Company management wants a solution that automatically responds to such events. Which solution meets these requirements?

- A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Setup AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Correct Answer: A

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results. A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.
- C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.
- D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on-demand capacity scaling enabled.

Correct Answer: B

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

- A. Modify the shipping application to write to a local database.
- B. Modify the application APIs to run serverless using AWS Lambda
- C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
- D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

Correct Answer: A

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB.
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

Correct Answer: C

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
- D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Correct Answer: C

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
- B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.

- C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
- D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Correct Answer: D

A web application must persist order data to Amazon S3 to support near-real time processing. A solutions architect needs to create an architecture that is both scalable and fault tolerant.

Which solutions meet these requirements? (Choose two.)

- A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Correct Answer: BE

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions. To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.

What should a solutions architect do to accomplish this?

- A. Create a NAT gateway and update the route table of the EC2 instances' subnet.
- B. Create a VPC endpoint and update the route table of the EC2 instances' subnet.
- C. Create a VPN connection and update the route table of the EC2 instances' subnet.
- D. Create a VPC peering connection and update the route table of the EC2 instances' subnet.

Correct Answer: D

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.

Which application change should a solutions architect recommend to resolve these issues?

- A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
- B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
- C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
- D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

Correct Answer: C

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year. Which solution meets these requirements and is the MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Correct Answer: D

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's .NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

- A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.
- B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
- C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

Correct Answer: B

A company has an application running on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3. To reduce costs, the company wants to configure its AWS resources in a cost-effective manner.

How should the company accomplish this?

- A. Deploy a NAT gateway to access the S3 buckets.

- B. Deploy AWS Storage Gateway to access the S3 buckets.
- C. Deploy an S3 gateway endpoint to access the S3 buckets.
- D. Deploy an S3 interface endpoint to access the S3 buckets.

Correct Answer: *B*

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment.

What should a solutions architect recommend?

- A. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
- B. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
- D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Correct Answer: *B*

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solutions architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

- A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
- B. Build the application to use Amazon Lightsail with On-Demand Instances.
- C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.
- D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

Correct Answer: *D*

A company is using Site-to-Site VPN connections for secure connectivity to its AWS Cloud resources from on-premises. Due to an increase in traffic across the VPN connections to the Amazon EC2 instances, users are experiencing slower VPN connectivity. Which solution will improve the VPN throughput?

- A. Implement multiple customer gateways for the same network to scale the throughput.

- B. Use a transit gateway with equal cost multipath routing and add additional VPN tunnels.
- C. Configure a virtual private gateway with equal cost multipath routing and multiple channels.
- D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

Correct Answer: A

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots replication and sub-millisecond response times.

What should the solutions architect recommend to solve these issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Correct Answer: B

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.
- B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Correct Answer: C

A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy.
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

Correct Answer: *A*

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data centre. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Answer(s): A

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners.

Which solution meets these requirements?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.
- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3

Answer(s): A

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution[^] but wants to further reduce data transfer costs. The company cannot modify the application's source code.

What should a solutions architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Answer(s): C

A company receives data from millions of users totalling about 1 TB each day. The company providers its users with usage report going back 12 months. All usage data must be stored for at least 5 years to comply with regularly and auditing requirement?

Which storage solution is MOST cost-effective?

- A. Store the data in Amazon S3 Standard Set a lifecycle rule to transition the data to S3 Glacier Deep after 1 year. Set a lifecycle rule to delete the data after 5 years.
- B. Store the data in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) Set a lifecycle rule to transition the data to S3 Glacier after 1 year set the lifecycle rule to delete the data after 5 years.

- C. Store the data in Amazon Standard Set a lifecycle rule to transmission the data to S3 Standard-infrequency Access (S3 Standard-IA) after 1 year Set a lifecycle rule to delete the data after 5 years.
- D. Store the data in Amazon S3 Standard Set a lifecycle rule to transition the data to S3 Zone-Infrequent Access (S3 One Zones-IA) after 1 year. Set a lifecycle rule to delete the data after 5 years.

Answer(s): A

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services. Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Answer(s): A

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

Answer(s): C

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.

Which solution meets these requirements MOST cost-effectively?

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

Answer(s): A

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow. Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register the instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Answer(s): A

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Answer(s): B

A company has applications that are deployed in multiple AWS Regions. The applications use an architecture that is based on Amazon EC2, Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), and Amazon DynamoDB.

The company lacks a mechanism for centralized data backup. A solutions architect must centralize data backup with the least possible operational effort.

What should the solutions architect do to meet these requirements?

- A. Tag all resources by project. Use AWS Systems Manager to set up snapshots by project and set DynamoDB incremental backups.
- B. Tag all resources by project. Create backup plans in AWS Backup to back up the data by tag name according to each project's needs.
- C. Tag all resources by project. Create an AWS Lambda function to run on schedule and take snapshots of each EC2 instance, EBS volume, and EFS file system by project. Configure the function to invoke DynamoDB on-demand backup.
- D. Use AWS CloudFormation to create a template for every new project so that all resources can be recreated at any time. Set the template to take daily snapshots of each EC2 instance, EBS volume, and EFS file system. Set the template to use DynamoDB on-demand backup for daily backups.

Answer(s): B

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-aci header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side- encryption header set.

Answer(s): D

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and an Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Answer(s): A

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

- A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
- D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Answer(s): C

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

- A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
- B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
- C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.
- D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Answer(s): C

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF. How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Answer(s): B

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Answer(s): A

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application

to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

- A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
- B. Create an AWS Step Functions workflow Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.
- C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.
- D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Answer(s): A

A solutions architect must transfer 750 TB of data from an on-premises network-attached file system to Amazon S3 Glacier. The migration must not saturate the on-premises 10 Mbps internet connection.

Which solution will meet these requirements?

- A. Create an AWS Site-to-Site VPN tunnel to an S3 bucket Transfer the files directly by using the AWS CLI.
- B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to an S3 bucket, and copy the files directly. Create an S3 Lifecycle policy to transition the S3 objects to S3 Glacier.
- D. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 bucket as the destination. Create an S3 Lifecycle policy to transition the S3 objects to S3 Glacier.

Answer(s): D

A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application's code.

Which solution meets these requirements?

- A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
- B. Servers.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
- D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

Answer(s): C

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train

other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Answer(s): B

A company is launching a new application that will be hosted on Amazon EC2 instances. A solutions architect needs to design a solution that does not allow public IPv4 access that originates from the internet. However, the solution must allow the EC2 instances to make outbound IPv4 internet requests.

The initial design proposal shows that the EC2 instances would be located in two private subnets across two Availability Zones. The entire architecture must be highly available.

How should the solutions architect change the architecture to meet these requirements?

- A. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.
- B. Deploy an internet gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.
- C. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.
- D. Deploy an egress-only internet gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.

Answer(s): C

A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

- A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
- B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
- C. Use Amazon CloudFront. Provide signed URLs to stream content.
- D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

Answer(s): C

A company stores project information in a shared spreadsheet. The company wants to create a web application to replace the spreadsheet. The company has chosen Amazon DynamoDB to store the spreadsheet's data and is designing the web application to display the project information that is obtained from DynamoDB.

A solutions architect must design the web application's backend by using managed services that require minimal

operational maintenance.

Which architectures meet these requirements? (Select TWO.)

- A. An Amazon API Gateway REST API accesses the project information that is in DynamoDB.
- B. An Elastic Load Balancer forwards requests to a target group with DynamoDB set up as the target.
- C. An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function accesses DynamoDB.
- D. An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that accesses DynamoDB.
- E. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that accesses DynamoDB.

Answer(s): A,E

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic.
- B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
- C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Answer(s): A

A healthcare computer stores highly sensitive records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and thin within 4 hours of a request thereafter.

What should a solutions architect recommend?

- A. Use Amazon S3 with cross-Region Region replication enabled. After 30 days. Transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CCRS) enabled. After 30 days. Transition on the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-origin replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive a lifecycle policy.
- D. Use Amazon S3 with cross-origin resource sharing (CCRS) enabled. After 30 days, transition on the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Answer(s): C

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process. The company's network team has ruled out bandwidth as a limiting factor.

Which actions should the solutions architect take to speed up the migration? (Select TWO.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

Answer(s): C,D

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an NFS protocol and must also be accessible from the AWS Cloud for further analytics and batch processing.

Which solution will meet these requirements?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS: then perform analytics on this data in the AWS Cloud.
- B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS. then perform analytics on this data in the AWS Cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud.

Answer(s): A

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynam
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Answer(s): A

A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward. The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application. The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.

The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs. What should a solutions architect recommend to meet these requirements?

- A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
- B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.

- C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.
- D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

Answer(s): B

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Answer(s): C

A computer is reviewing a recent migration of a three-tier application to a VPC. The security team discover that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solution architect do to connect issue?

- A. Create security group rules using the instance ID as the source destination.
- B. Create security group rules using the security ID as the source or destination.
- C. Create security group rules using the VPC CDR blocks as the source or destination.
- D. Create security group rules using the subnet CDR blocks as the source or destination.

Answer(s): C

A company is using AWS Key Management Service (AWS KMS) customer master keys (CMKs) to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Select TWO.)

- A. Add AWS KMS permissions in the Lambda resource policy
- B. Add AWS KMS permissions in the Lambda execution role
- C. Add AWS KMS permissions in the Lambda function policy.
- D. Allow the Lambda execution role in the AWS KMS key policy.
- E. Allow the Lambda resource policy in the AWS KMS key policy.

Answer(s): B,C

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest. Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Answer(s): D

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

Answer(s): D

A company is automating an order management application. The company's development team has decided to use SFTP to transfer and store the business-critical information files. The files must be encrypted and must be highly available. The files also must be automatically deleted a month after they are created.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply an AWS Transfer for SFTP file retention policy to delete the files after a month.
- B. Install an SFTP service on an Amazon EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file share on the EC2 instance. Enable cron to delete the files after a month.
- C. Configure an Amazon Elastic File System (Amazon EFS) file system with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the EFS file system. Apply an EFS lifecycle policy to automatically delete the files after a month.
- D. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply S3 Lifecycle rules to automatically delete the files after a month.

Answer(s): D

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages
Configure the EC2 instance to save the results to an Amazon S3 bucket.
- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer(s): B

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Select TWO.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.

Answer(s): A,D

A company hosts an application on AWS. The application interacts with an Amazon DynamoDB table that has 10 read capacity units (RCUs). Data from Amazon CloudWatch alarms shows that throttling is occurring on read requests to the DynamoDB table. The company needs to prevent this issue from happening in the future as the application continues to grow.

What should a solutions architect recommend to meet these requirements?

- A. Add an Elastic Load Balancer in front of the DynamoDB table.
- B. Change the RCUs for the DynamoDB table to 20.
- C. Provision 20 write capacity units (WCUs) for the DynamoDB table to offset the throttling on read requests.
- D. Enable auto scaling for the DynamoDB table.

Answer(s): D

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently. What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Answer(s): A

A company has a custom application running on an Amazon EC2 instance that:

- Reads a large amount of data from Amazon S3
- Performs a multi-stage analysis.

Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis. The process performance depends on the temporary storage performance. What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Answer(s): A

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer(s): C

A company needs to store 160TB of data for an indefinite of time. The company must be able to use standard SQL and business intelligence tools to query all of the data. The data will be queried no more than twice each month.

What is the MOST cost-effective solution that meets these requirements?

- A. Store the data in Amazon Aurora Serverless with MySQL. Use an SQL client to query the data.

- B. Store the data in Amazon S3. Use AWS Glue, Amazon Athena, IDBC and COBC drivers to query the data.
- C. Store the data in an Amazon EMR cluster with EMR File System (EMRFS) as the storage layer use Apache Presto to query the data.
- D. Store a subset of the data in Amazon Redshift, and store the remaining data in Amazon S3. Use Amazon Redshift Spectrum to query the S3 data.

Answer(s): D

A solution architect at a company is designing the architecture for a two-tiered web application. The web application is composed of an internet facing application load balancer that forwards traffic to an auto scaling group of Amazon EC2 instances. The EC2 instances must be able to access a database that runs on Amazon RDS.

The company has requested a defence-in-depth approach to the network layout. The company does not want to rely solely on security groups or network ACLs. Only the minimum resources that are necessary should be routable from the internet.

Which network design should the solutions architect recommend to meet these requirements?

- A. Place the ALB, EC2 instances and RDS database in private subnets.
- B. Place the ALB in public subnets. Place the EC2 instances and RDS database in private subnets.
- C. Place the ALB and EC2 instances in public subnets. Place the RDS database in private subnets.
- D. Place the ALB outside the VPC. Place the EC2 instances and RDS database in private subnets.

Answer(s): C

The application's traffic is often low, but it occasionally grows significantly. During these sudden increases in traffic, DynamoDB returns throttling errors. The result is that error pages are displayed to end users.

What should a solutions architect do to reduce these errors?

- A. Change the DynamoDB table to use on-demand capacity mode.
- B. Create a DynamoDB read replica to scale the read traffic horizontally.
- C. Purchase DynamoDB reserved capacity of 1,000 RCU and 500 WCU.
- D. Configure the application to use strongly consistent reads for DynamoDB queries.

Answer(s): D

A solutions architect is designing the architecture for a company website that is composed of static content. The company's target customers are located in the United States and Europe.

Which architecture should the solutions architect recommend to MINIMIZE cost?

- A. Store the website files on Amazon S3 in the us-east-2 Region. Use an Amazon CloudFront distribution with the price class configured to limit the edge locations in use.
- B. Store the website files on Amazon S3 in the us-east-2 Region. Use an Amazon CloudFront distribution with the price class configured to maximize the use of edge locations.
- C. Store the website files on Amazon S3 in the us-east-2 Region and the eu-west-1 Region. Use an Amazon CloudFront geolocation routing policy to route requests to the closest Region to the user.
- D. Store the website files on Amazon S3 in the us-east-2 Region and the eu-west-1 Region. Use an Amazon CloudFront distribution with an Amazon Route 53 latency routing policy to route requests to the closest Region to the user.

Answer(s): D

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

- A. Configure Amazon Route 53 health checks for each Region. Use an active-active failover configuration.
- B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.
- C. Create an AWS Transit Gateway Attach the transit gateway to the API Gateway endpoint in each Region Configure the transit gateway to route requests.
- D. Use AWS Global Accelerator to create an accelerator with endpoints in each Region. Allow Global Accelerator to automatically monitor the health of endpoints and route requests.

Answer(s): A

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

- A. Create an SQS dead-letter queue Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Answer(s): B

A company needs a storage solution for an application that runs on a high performance computing (HPC) cluster. The cluster is hosted on AWS Fargate for Amazon Elastic Container Service (Amazon ECS). The company needs a mountable file system that provides concurrent access to files while delivering hundreds of GBps of throughput at sub-millisecond latencies.

Which solution meets these requirements?

- A. Create an Amazon FSx for Lustre file share for the application data Create an IAM role that allows Fargate to access the FSx for Lustre file share.
- B. Create an Amazon Elastic File System (Amazon EFS) file share for the application data. Create an IAM role that allows Fargate to access the EFS file share.
- C. Create an Amazon S3 bucket for the application data. Create an S3 bucket policy that allows Fargate to access the S3 bucket.
- D. Create an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io2) volume for the application data Create an IAM role that allows Fargate to access the volume.

Answer(s): A

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "1",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        }  
    ]  
}
```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2 StopInstances and ec2.TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2 StopInstances and ec2.TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Answer(s): D

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company's IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.

What should a solutions architect do to secure the data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Answer(s): D

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing.

Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Answer(s): A

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions

architect must design the most operationally efficient process for image uploads.

Which combination of actions should the solutions architect take to meet these requirements? (Select TWO.)

- A. Configure the application to upload images to S3 Glacier.
- B. Configure the web server to upload the original images to Amazon S3.
- C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Answer(s): D,E

A company captures ordered clickstream data from multiple websites and uses batch processing to analyze the data. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data.

The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.

Which combination of AWS services will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer(s): B,C

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

What should the solutions architect do to meet this requirement?

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

Answer(s): B

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and context daily, but have been complaining of timeout. The architect uses Amazon EC2 Auto Scaling groups, and

the custom application consistently takes 1 minutes to initiate upon boot up before responding to user requests. How should a solutions architect redesign the architect to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Answer(s): C

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

- A. Upload files from the user's browser to the application servers Transfer the files to an Amazon S3 bucket.
- B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.
- C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

Answer(s): C

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS. However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.
- C. Build a database cache using Amazon ElastiCache.
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Answer(s): C

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

- A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.

- B. Configure a backup window for the RDS DB Instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
- C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
- D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Answer(s): A

A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

- A. Use AWS Snowball Edge devices to process and store the images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.
- D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Answer(s): A

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement, and support the NFS protocol.

Which solution meets these requirements?

- A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
- B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the instances and apply that to the additional instance.
- C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 instances that need access to the data.
- D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Answer(s): A

A manufacturing company has machine sensors that upload csv files to an Amazon S3 bucket. These csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the csv files must be kept to train machine learning (ML)

models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO)

- A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
- B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket Invoke the Lambda function when a csv file is uploaded.
- C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket Transition the csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.
- D. Create S3 Lifecycle rules for csv files and image files in the S3 bucket Transition the csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploaded Expire the image files after 30 days.
- E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Answer(s): B,D

A company is developing a serverless web application that gives users the ability to interact with real-time analytics from online games. The data from the games must be streamed in real time. The company needs a durable, low-latency database option for user data. The company does not know how many users will use the application Any design considerations must provide response times of single-digit milliseconds as the application scales.

Which combination of AWS services will meet these requirements? (Select TWO.)

- A. Amazon CloudFront
- B. Amazon DynamoDB
- C. Amazon Kinesis
- D. Amazon RDS
- E. AWS Global Accelerator

Answer(s): B,C

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials needs to be removed from the Lambda source code. The credentials must then be securely stored and rotated on a on-going basis to meet security policy requirements.

What should a solutions architect recommend meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can review the password from CloudHSM given key ID.
- B. Store the password in AWS Secrets Manager . A associate the Lambda function with a role that can retrieve the password from secrets Manager given its secret ID.
- C. Move the database password to an environment variable associate the Lambda function Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key I

Answer(s): B

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

- A. Add an Amazon Inspector agent to the ALB
- B. Configure Amazon CloudFront to prevent attacks.
- C. Enable AWS Shield Advanced to prevent attacks.
- D. Configure Amazon GuardDuty to monitor the ALB

Answer(s): C

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer(s): C

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Select TWO.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- C. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- D. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Answer(s): A,B

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.

What should a solutions architect do to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check.
- C. Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Answer(s): B

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses a customer managed customer master key (CMK) to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

- A. Make the encrypted AMI and snapshots publicly available. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.
- B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.
- C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.
- D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account. Encrypt the S3 bucket with a CMK that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

Answer(s): B

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However many of the web service clients can only reach IP addresses whitelisted on their firewalls. What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address.
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer(s): A

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead for managing and scaling the database must be minimized.

Which database solution should the solutions architect recommend?

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

Answer(s): B

A solutions architect is designing the cloud architecture for a new application that is being deployed on AWS. The application's users will interactively download and upload files. Files that are more than 90 days old will be accessed less frequently than newer files, but all files need to be instantly available. The solutions architect must

ensure that the application can scale to store petabytes of data with maximum durability.
Which solution meets these requirements?

- A. Store the files in Amazon S3 Standard. Create an S3 Lifecycle policy that moves objects that are more than 90 days old to S3 Glacier.
- B. Store the tiles in Amazon S3 Standard. Create an S3 Lifecycle policy that moves objects that are more than 90 days old to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data that is more than 90 days old.
- D. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data that is more than 90 days old.

Answer(s): B

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer(s): A

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

Answer(s): A

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solution architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM across all accounts in the organizational unit.

- C. Prevent the developers from attaching any policies and duties to the security option team.
- D. Set an IAM permission boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Answer(s): D

A company needs to connect its on-premises data center network to a new VPC. The data center network has a 100 Mbps symmetrical internet connection. An application that is running on premises will transfer multiple gigabytes of data each day. The application will use an Amazon Kinesis Data Firehose delivery stream for processing.

What should a solutions architect recommend for maximum performance?

- A. Create a VPC peering connection between the on-premises network and the VPC Configure routing for the on-premises network to use the VPC peering connection.
- B. Procure an AWS Snowball Edge Storage Optimized device. After several days' worth of data has accumulated, copy the data to the device and ship the device to AWS for expedited transfer to Kinesis Data Firehose Repeat as needed.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the VPC Configure BGP routing between the customer gateway and the virtual private gateway. Use the VPN connection to send the data from on premises to Kinesis Data Firehose.
- D. Use AWS PrivateLink to create an interface VPC endpoint for Kinesis Data Firehose in the VPC. Set up a 1 Gbps AWS Direct Connect connection between the on-premises network and AWS Use the PrivateLink endpoint to send the data from on premises to Kinesis Data Firehose.

Answer(s): D

A company is hosting an application in its own data center. The application uses Amazon S3 for data storage. The application transfers several hundred terabytes of data every month to and from Amazon S3. The company needs to minimize the cost of this data transfer.

Which solution meets this requirement?

- A. Establish an AWS Direct Connect connection between the AWS Region in use and the company's data center Route traffic to Amazon S3 over the Direct Connect connection.
- B. Establish an AWS Site-to-Site VPN connection between the company's data center and a VPC in the AWS Region in use. Create a VPC endpoint for Amazon S3 in the VPC. Route traffic to Amazon S3 over the VPN connection to the S3 endpoint.
- C. Create an AWS Storage Gateway file gateway Deploy the software appliance in the company's data center Configure the application to use the file gateway to store and retrieve files.
- D. Create an FTPS server by using AWS Transfer Family. Configure the application to use the FTPS server to store and retrieve files.

Answer(s): C

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

Answer(s): C

An ecommerce company is creating an application that requires a connection to a third-party payment service to process payments. The payment service needs to explicitly allow the public IP address of the server that is making the payment request. However, the company's security policies do not allow any server to be exposed directly to the public internet.

Which solution will meet these requirements?

- A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.
- B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.
- C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.
- D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

Answer(s): C

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Answer(s): B

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.

- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance.
Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance.
Modify the game to use Redis.

Answer(s): D

A company is designing a new application that runs in a VPC on Amazon EC2 instances. The application stores data in Amazon S3 and uses Amazon DynamoDB as its database. For compliance reasons, the company prohibits all traffic between the EC2 instances and other AWS services from passing over the public internet. What can a solutions architect do to meet this requirement?

- A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB
- B. Configure interface VPC endpoints to Amazon S3 and DynamoDB
- C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.
- D. Configure a gateway VPC endpoint to DynamoDB Configure an interface VPC endpoint to Amazon S3

Answer(s): A

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database.

What should the solutions architect do to ensure that the website can scale with increasing traffic? (Select TWO.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Answer(s): A,B

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts. Which AWS service can the administrator use to protect the company against attacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

Answer(s): B

A company must migrate 20 TB of data from a data centre to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization.

What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration

Answer(s): A

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Answer(s): D

A company is running a web application on Amazon EC2 instances in an Auto Scaling group. The application uses a database that runs on an Amazon RDS for PostgreSQL DB instance. The application performs slowly as traffic increases, and the database experiences a heavy read load during periods of high traffic.

Which actions should a solutions architect take to resolve these performance issues? (Select TWO.)

- A. Enable auto scaling for the DB instance.
- B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.
- C. Enable Multi-AZ for the DB instance. Configure the application to send read traffic to the standby DB instance.
- D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.
- E. Configure the Auto Scaling group subnets to ensure that the EC2 instances are provisioned in the same Availability Zone as the DB instance.

Answer(s): B,D

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer(s): C,D

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.

Which storage solution meets these requirements?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Answer(s): B

A company has three VPCs named Development, Testing and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Answer(s): D

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Select TWO.)

- A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
- B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
- D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue Set the message attribute to use the payment ID
- E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Answer(s): A,E

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Answer(s): C

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However, the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group.
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica.
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Answer(s): C

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a

period of time during surges A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

Answer(s): D

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls. What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address.
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

Answer(s): A

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

- A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
- B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
- C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
- D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Answer(s): A

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.

What should the solutions architect do to meet these requirements?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Answer(s): D

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images. Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Answer(s): B

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer(s): A

A solution architect is designing a new service behind API Gateway. The request pattern for the service will be unpredictable and can change suddenly from 0 request to over 500 per second. The total size of the data that needs to be persisted database is currently less than 1 GB and is expected to grow unpredictably. Data can be queried using sampling key -value request.

Which combination of AWS services would meet these requirements? (Select TWO.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer(s): A,C

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Answer(s): D

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

- D. Create an A record in a Route 53 hosted zone for the application Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Answer(s): B

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.

Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

Deploy a NAT instance in a private subnet of each Availability Zone.

Deploy a NAT gateway in a public subnet of each Availability Zone.

Deploy a transit gateway in a private subnet of each Availability Zone.

Deploy an internet gateway in a public subnet of each Availability Zone.

Answer(s): B

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

- A. Add AWS Shield
- B. Add Aurora Replicas.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Answer(s): B,E

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS

Answer(s): B

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversion.

What should a solutions architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.
- D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Answer(s): D

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance Store process, and delete the messages., respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process, integrate the sender application to write to the SNS topic.

Answer(s): C

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is shared across a cluster of Linux servers. The company wants to reduce storage costs for the application.

What should a solutions architect do to meet these requirements?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon EFS and store them locally on each Amazon EC2 instance.
- C. Configure a lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
- D. Move the files to Amazon S3 with S3 Lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

Answer(s): C

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

Which storage solution meets these requirements MOST cost-effectively?

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

Answer(s): D

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be need with as little latency as possible. A possible architect needs design an optimal solution that requires minimal application changes.

Which method should the solution architect select?

- A. Configure amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read lead the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB.
Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint of DynamoDB.

Answer(s): A

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to fail over to us-west-2 with a recovery time objective (RTO) of 15 minutes.

What should a solutions architect recommend to meet these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Answer(s): B

A company processes large amounts of data. The output data is stored in Amazon S3 Standard storage in an S3 bucket, where it is analyzed for 1 month. The data must remain immediately accessible after the 1-month analysis period.

Which storage solution meets these requirements MOST cost-effectively?

- A. Configure an S3 Lifecycle policy to transition the objects to S3 Glacier after 30 days.
- B. Configure S3 Intelligent-Tiering to transition the objects to S3 Glacier after 30 days.
- C. Configure an S3 Lifecycle policy to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Configure an S3 Lifecycle policy to delete the objects after 30 days. Enable versioning on the S3 bucket so that deleted objects can still be immediately restored as needed.

Answer(s): B

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone- IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard- IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Answer(s): D

A company is developing a new online gaming application. The application will run on Amazon EC2 instances in multiple AWS Regions and will have a high number of globally distributed users. A solutions architect must design the application to optimize network latency for the users.

Which actions should the solutions architect take to meet these requirements? (Select TWO.)

- A. Configure AWS Global Accelerator. Create Regional endpoint groups in each Region where an EC2 fleet is hosted.
- B. Create a content delivery network (CDN) by using Amazon CloudFront. Enable caching for static and dynamic content, and specify a high expiration period.
- C. Integrate AWS Client VPN into the application. Instruct users to select which Region is closest to them after they launch the application. Establish a VPN connection to that Region.
- D. Create an Amazon Route 53 weighted routing policy. Configure the routing policy to give the highest weight to the EC2 instances in the Region that has the largest number of users.
- E. Configure an Amazon API Gateway endpoint in each Region where an EC2 fleet is hosted. Instruct users to select which Region is closest to them after they launch the application. Use the API Gateway endpoint that is closest to them.

Answer(s): A,B

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.

How should the company deploy this solution?

- A. Use Amazon S3 website hosting for the backup website and a Route 53 failover routing policy.
- B. Use Amazon S3 website hosting for the backup website and a Route 53 latency routing policy.
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
- D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Answer(s): A

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Answer(s): C

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs.

What should a solutions architect recommend to accomplish this?

- A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
- B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic Kubernetes Service (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
- C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda function for the application layer. Use Amazon DynamoDB to store user data.
- D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda function for the application layer. Use Amazon RDS with read replicas to store user data.

Answer(s): C

A company has an on-premises application that collects data and stores it to an on-premises NFS server. The company recently set up a 10 Gbps AWS Direct Connect connection. The company is running out of storage capacity on-premises. The company needs to migrate the application data from on-premises to the AWS Cloud while maintaining low-latency access to the data from the on-premises application.

What should a solutions architect do to meet these requirements?

- A. Deploy AWS Storage Gateway for the application data and use the file gateway to store the data in Amazon S3 Connect the on-premises application servers to the file gateway using NFS
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS
- C. Configure AWS Storage Gateway as a volume gateway Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store {Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer Connect the on-premises application to the EFS file system.

Answer(s): D

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

Which combination of actions should a solutions architect take to meet these requirements⁷ (Select TWO.)

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Answer(s): B,D

A solutions architect needs to design a highly available application consisting of web, application and database tiers HTTPS content delivery should be as close to the edge as possible with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer(s): B

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

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

Answer(s): D

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Answer(s): A

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

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

Answer(s): D

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority.

Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store.
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume.
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled.
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled.

Answer(s): A

A company is building a web application that serves a content management system. The content management system runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across multiple Availability Zones. Users are constantly adding and updating files, blogs, and other website assets in the content management system.

A solutions architect must implement a solution in which all the EC2 instances share up-to-date website content with the least possible lag time.

Which solution meets these requirements?

- A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently. Configure the ALB to make changes to the website assets only in the newest EC2 instance.
- B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system. Configure each EC2 instance to mount the EFS file system locally. Configure the website hosting application to reference the website assets that are stored in the EFS file system.
- C. Copy the website assets to an Amazon S3 bucket. Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume. Run the S3 sync command once each hour to keep files up to date.
- D. Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets. Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched. Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume.

Answer(s): B

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migration?

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

Answer(s): C

A company has an Amazon S3 bucket that contains mission-critical data. The company wants to ensure this data is protected from accidental deletion. The data should still be accessible, and a user should be able to delete the data internationally.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Answer(s): A,B

A company build an application that gives users the ability to check in to places they visit, rank the places, and add reviews about their experiences. The application is successful and is experiencing a rapid increase in the number of users every month.

The company uses a single Amazon RDS for MySQL DB instance for its database. The company fears that the database might not be able to handle the load for the upcoming month because the DB instance has activated alarms that are related to resource exhaustion.

A solutions architect must design a solution that prevents service interruptions at the database layer. The solutions architect also must minimize any changes to code.

Which solution meets these requirements?

- A. Create RDS read replicas. Redirect read-only traffic to the read replica endpoints.
- B. Create an Amazon EMR cluster. Migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster. Redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Turn on the Multi-AZ feature for the DB instance. Redirect read-only traffic to the standby replica endpoint.

Answer(s): A

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection to the bastion host and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Answer(s): B,E

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order two microservices should handle the event simultaneously. The Email microservice will send a confirmation email and the OrderProcessing microservice will start the order delivery process. If a customer cancels an order, the OrderCancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple

Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

- A. Create a single SQS queue and publish order events to it The Email, OrderProcessing and OrderCancellation microservices can then consume messages off the queue.
- B. Create three SNS topics for each microservice Publish order events to the three topics Subscribe each of the Email OrderProcessmg, and OrderCancellation microservices to its own topic.
- C. Create an SNS topic and publish order events to it Create three SQS queues for the Email OrderProcessing and OrderCancellation microservices Subscribe all SQS queues to the SNS topic with message filtering.
- D. Create two SQS queues and publish order events to both queues simultaneously One queue is for the Email and OrderProcessmg microservices The second queue is for the Email and Order Cancellation microservices.

Answer(s): C

A solutions architect is optimizing a website for an upcoming musical event Videos of the performances will be streamed in real time and then will be available on demand The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

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

Answer(s): A

A company wants lo share data that is collected from sell-driving cars with the automobile community. The data will be made available (rom within an Amazon S3 bucket. The company wants to minimize its cost of making this data available to other AWS accounts.

What should a solutions architect do to accomplish this goal?

- A. Create an S3 VPC endpoint for the bucket.
- B. Configure the S3 bucket to be a Requester Pays bucket.
- C. Create an Amazon CloudFront distribution in front of the S3 bucket.
- D. Require that the fries be accessible only with the use of the BitTorrent protocol.

Answer(s): A

A company has a website hosted on AWS The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.

What should a solutions architect do to meet this requirement?

- A. Update the ALB's network ACL to accept only HTTPS traffic.
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Answer(s): C

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

- A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
- B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
- C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
- D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route traffic to the ALB from Route 53.

Answer(s): D

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Answer(s): C

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier connects with the RDS instance. There are frequent calls to return identical database from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElasticCache to cache the large database.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer(s): B

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks. Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL (or the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Answer(s): C

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Answer(s): D

A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network. However, the company does not want users to have to maintain another identity to access the resources. A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources. What should the solutions architect do to meet these requirements?

- A. Create an IAM user for each user in the company. Attach the appropriate policies to each user.
- B. Use Amazon Cognito with an Active Directory user pool. Create roles with the appropriate policies attached.
- C. Define cross-account roles with the appropriate policies attached. Map the roles to the Active Directory groups.
- D. Configure Security Assertion Markup Language (SAML) 2.0-based federation. Create roles with the appropriate policies attached. Map the roles to the Active Directory groups.

Answer(s): D

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the Add Permission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Answer(s): D

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only. What should a solutions architect do to protect against data loss? (Select TWO.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Answer(s): A,E

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

Answer(s): D

A disaster relief company is designing a new solution to analyze real-time csv data. The data is collected by a network of thousands of research stations and are distributed across the world. The data volume is consistent and constant, and the size of each data file is 512 KB. The company needs to stream the data and analyze the data in real time.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Provision an appropriately sized Amazon Simple Queue Service (Amazon SQS) queue. Use the AWS SDK at the research stations to write the data into the SQS queue.

- B. Provision an appropriately sized Amazon Kinesis Data Firehose delivery stream. Use the AWS SDK at the research stations to write the data into the delivery stream and then into an Amazon S3 bucket.
- C. Provision an appropriately sized Amazon Kinesis Data Analytics application. Use the AWS CLI to configure Kinesis Data Analytics with SQL queries.
- D. Provision an AWS Lambda function to process the data. Set up the BatchSize property on the Lambda event source.
- E. Provision an AWS Lambda function to process the data. Set up an Amazon EventBridge (Amazon CloudWatch Events) cron expression rule to invoke the Lambda function.

Answer(s): A,D

A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.

Which combination of actions should the company take to meet these requirements? (Select TWO.)

- A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Answer(s): A,D

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Answer(s): A,B

A company runs an AWS Lambda function in private subnets in a VPC. The subnets have a default route to the internet through an Amazon EC2 NAT instance. The Lambda function processes input data and saves its output as an object to Amazon S3. Intermittently, the Lambda function times out while trying to upload the object because of saturated traffic on the NAT instance's network. The company wants to access Amazon S3 without traversing the internet.

Which solution will meet these requirements?

- A. Replace the EC2 NAT instance with an AWS managed NAT gateway.
- B. Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type.

- C. Provision a gateway endpoint for Amazon S3 in the VPC Update the route tables of the subnets accordingly.
- D. Provision a transit gateway Place transit gateway attachments in the private subnets where the Lambda function is running.

Answer(s): C

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Answer(s): B

A company is running a multi-tier web application on AWS. The application runs its database on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region.

A database administrator who monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica. The result is increased read latency for the application. The memory and disk utilization of the DB instance are stable throughout the event of increased latency.

What should a solutions architect do to improve the read scalability?

- A. Reboot the DB cluster
- B. Create a cross-Region read replica
- C. Configure Aurora Auto Scaling for the read replica
- D. Increase the provisioned read IOPS for the DB instance

Answer(s): B

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC

Answer(s): A

A solutions architect is designing a multi-Region disaster recovery solution (or an application that will provide public API access). The application will use Amazon EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost/?

- A. Use an Application Load Balancer for Region failover Deploy new EC2 instances with the userdata script Deploy separate RDS instances in each Region.
- B. Use Amazon Route 53 for Region failover Deploy new EC2 instances with the userdata script Create a read replica of the RDS instance in a backup Region.
- C. Use Amazon API Gateway for the public APIs and Region failover Deploy new EC2 instances with the userdata script Create a MySQL read replica of the RDS instance in a backup Region.

- D. Use Amazon Route 53 for Region failover Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup Replicate the snapshot to a backup Region.

Answer(s): C

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.

What should a solutions architect do to minimize the anticipated server load?

- A. Store the videos in Amazon ElastiCache for Redis Update the web servers to serve the videos using the ElastiCache API
- B. Store the videos in Amazon Elastic File System (Amazon EFS) Create a user data script for the web servers to mount the EFS volume.
- C. Store the videos in an Amazon S3 bucket Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket Restrict Amazon S3 access to the OAI.
- D. Store the videos in an Amazon S3 bucket Create an AWS Storage Gateway file gateway to access the S3 bucket Create a user data script for the web servers to mount the file gateway.

Answer(s): C

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited Enable provisioned retrieved capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage GATEWAY store data in Amazon retaining copies of frequently accessed data subnets locally.
- C. Deploy AWS Storage gateway using stored volume to store data locally Use Storage gateway asynchronously back up point-in-time snapshots of the data Amazon S3.
- D. Deploy AWS Direct Connect to connect with on-premises data center. Configure AWS Storage gateway to store data locally use storage gateway to asynchronously back up point-in-time snapshot of data Amazon S3.

Answer(s): B

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets Each private subnet uses a NAT instance for Internet access All images are stored in Amazon S3 buckets The company is concerned about the data transfer costs between Amazon ECS and Amazon S3

What should a solutions architect do to reduce costs?

- A. Configure a NAT gateway to replace the NAT instances.
- B. Configure a gateway endpoint for traffic destined to Amazon S3
- C. Configure an interface endpoint for traffic destined to Amazon S3
- D. Configure Amazon CloudFront for the S3 bucket storing the images.

Answer(s): C

A developer is creating an AWS Lambda function to perform dynamic updates to a database when an item is added to an Amazon Simple Queue Service (Amazon SOS) queue. A solutions architect must recommend a solution that tracks any usage of database credentials in AWS CloudTrail. The solution also must provide auditing capabilities.

Which solution will meet these requirements?

- A. Store the encrypted credentials in a Lambda environment variable
- B. Create an Amazon DynamoDB table to store the credentials. Encrypt the table
- C. Store the credentials as a secure string in AWS Systems Manager Parameter Store
- D. Use an AWS Key Management Service (AWS KMS) key store to store the credentials

Answer(s): D

A company uses on-premises servers to host its application. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

Which combination of actions should a solutions architect take to meet these requirements? (Select TWO.)

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway Me gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Answer(s): B,D

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Answer(s): C

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two Use Amazon Route 53 weighted record sets to distribute requests across instances.

Answer(s): A

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table.
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Answer(s): D

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS) The solutions architect has proposed migrating the MS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file share to Amazon RDS
- B. Migrate the file share to AWS Storage Gateway.
- C. Migrate the file share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Answer(s): C

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML) The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region The company hosts a web application that the customers use to purchase access to a given dataset The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer After a purchase is made customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

- A. Configure S3 Transfer Acceleration on the existing S3 bucket Direct customer requests to the S3 Transfer Acceleration endpoint Continue to use S3 signed URLs for access control.

- B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin Direct customer requests to the CloudFront URL Switch to CloudFront signed URLs for access control.
- C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets Direct customer requests to the closest Region Continue to use S3 signed URLs for access control.
- D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket Implement access control directly in the application.

Answer(s): B

A company has deployed a business-critical application in the AWS Good The application uses Amazon EC2 instances that run in the us-east-1 Region The application uses Amazon S3 for storage of all critical data. To meet compliance requirements the company must create a disaster recovery (DR) plan that provides the capability of a full failover to another AWS Region.

What should a solutions architect recommend for this DR plan?

- A. Deploy the application to multiple Availability Zones in us-east-1 Create a resource group in AWS Resource Groups Turn on automatic failover for the application to use a predefined recovery Region.
- B. Perform a virtual machine (VM) export by using AWS Import/Export on the existing EC2 instances Copy the exported instances to the destination Region in the event of a disaster provision new EC2 instances from the exported EC2 instances.
- C. Create snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instances in us-east-1 Copy the snapshots to the destination Region In the event of a disaster provision new EC2 instances from the EBS snapshots.
- D. Use S3 Cross-Region Replication for the data that is stored in Amazon S3 Create an AWS CloudFormation template for the application with an S3 bucket parameter In the event of a disaster deploy the template to the destination Region and specify the local S3 bucket as the parameter.

Answer(s): D

A company is using AWS to design a web application that will process insurance quotes Users will request quotes from the application Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost The solution must maximize operational efficiency and must minimize maintenance. Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type Configure the web application to send messages to the proper data stream Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pool messages from its own data stream.
- B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type Subscribe the Lambda function to its associated SNS topic Configure the application to publish requests tot quotes to the appropriate SNS topic.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type Configure each backend application server to use its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasucsearch Service (Amazon ES) cluster Configure the application to send

messages to the proper delivery stream Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

Answer(s): C

A company has a web application with sporadic usage patterns There is heavy usage at the beginning of each month moderate usage at the start of each week and unpredictable usage during the week The application consists of a web server and a MySQL database server running inside the data center The company would like to move the application to the AWS Cloud and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless.
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group.

Answer(s): B

A company is planning to store sensitive documents in an Amazon S3 bucket. The documents must be encrypted at rest. The company wants to manage the underlying keys that are used for encryption However, the company does not want to manage the encryption and decryption process.

Which solutions will meet these requirements? (Select TWO.)

- A. Use server-side encryption with customer-provided encryption keys (SSE-C).
- B. Use client-side encryption with AWS managed keys.
- C. Use server-side encryption with S3 managed encryption keys (SSE-S3).
- D. Use server-side encryption with AWS KMS managed encryption keys (SSE-KMS) with a key policy document that is 40 KB in size.
- E. Use server-side encryption with AWS KMS managed encryption keys (SSE-KMS) that the company uploads to AWS KMS.

Answer(s): C,E

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers In an Auto Scaling group Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Answer(s): B

A user wants to list the IAM role that is attached to their Amazon EC2 Instance. The user has login access to the EC2 instance but does not have IAM permissions. What should a solutions architect do to retrieve this information?

A)

Run the following EC2 command:

```
curl http://169.254.169.254/latest/meta-data/iam/info
```

B)

Run the following EC2 command:

```
curl http://169.254.169.254/latest/user-data/iam/info
```

C)

Run the following EC2 command:

```
http://169.254.169.254/latest/dynamic/instance-identity/
```

D)

Run the following AWS CLI command:

```
aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile
```

Answer(s): A

A company is building a new furniture inventory application. The company has deployed the application on a fleet of Amazon EC2 instances across multiple Availability Zones. The EC2 instances run behind an Application Load Balancer (ALB) in their VPC.

A solutions architect has observed that incoming traffic seems to favor one EC2 instance resulting in latency for some requests.

What should the solutions architect do to resolve this issue?

- A. Disable session affinity (sticky sessions) on the ALB
- B. Replace the ALB with a Network Load Balancer.
- C. Increase the number of EC2 instances in each Availability Zone.
- D. Adjust the frequency of the health checks on the ALB's target group.

Answer(s): B

An airline that is based in the United States provides services for routes in North America and Europe. The airline is developing a new read-intensive application that customers can use to find flights on either continent. The application requires strong read consistency and needs scalable database capacity to accommodate changes in user demand. The airline needs the database service to synchronize with the least possible latency between the two continents and to provide a simple failover mechanism to a second AWS Region.

Which solution will meet these requirements?

- A. Deploy Microsoft SQL Server on Amazon EC2 instances in a Region in North America. Use SQL Server binary log replication on an EC2 instance in a Region in Europe.
- B. Create an Amazon DynamoDB global table. Add a Region from North America and a Region from Europe to the table. Query data with strongly consistent reads.

- C. Use an Amazon Aurora MySQL global database. Deploy the read-write node in a Region in North America, and deploy read-only endpoints in Regions in North America and Europe. Query data with global read consistency.
- D. Create a subscriber application that uses Amazon Kinesis Data Streams for an Amazon Redshift cluster in a Region in North America. Create a second subscriber application for the Amazon Redshift cluster in a Region in Europe. Process all database modifications through Kinesis Data Streams.

Answer(s): C

A company wants to perform an online migration of active datasets from an on-premises NFS server to an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. Data integrity verification is required during the transfer and at the end of the transfer. The data also must be encrypted.

A solutions architect is using an AWS solution to migrate the data.

Which solution meets these requirements?

- A. AWS Storage Gateway file gateway
- B. S3 Transfer Acceleration
- C. AWS DataSync
- D. AWS Snowball Edge Storage Optimized

Answer(s): C

A company has an application that uses an Amazon OynamoDB table for storage. A solutions architect discovers that many requests to the table are not returning the latest data. The company's users have not reported any other issues with database performance. Latency is in an acceptable range.

Which design change should the solutions architect recommend?

- A. Add read replicas to the table.
- B. Use a global secondary index (GSI).
- C. Request strongly consistent reads for the table.
- D. Request eventually consistent reads for the table.

Answer(s): C

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Answer(s): A

A company has an Amazon S3 bucket that contains confidential information in its production AWS account. The company has turned on AWS CloudTrail for the account. The account sends a copy of its logs to Amazon CloudWatch Logs. The company has configured the S3 bucket to log read and write data events.

A company auditor discovers that some objects in the S3 bucket have been deleted A solutions architect must provide the auditor with information about who deleted the objects.

What should the solutions architect do to provide this information?

- A. Create a CloudWatch Logs filter to extract the S3 write API calls against the S3 bucket.
- B. Query the CloudTrail logs with Amazon Athena to identify the S3 write API calls against the S3 bucket.
- C. Use AWS Trusted Advisor to perform security checks for S3 write API calls that deleted the content.
- D. Use AWS Config to track configuration changes on the S3 bucket Use these details to track the S3 write API calls that deleted the content.

Answer(s): B

A company is running a three-tier web application to process credit card payments The front-end user interface consists of static webpages The application tier can have long-running processes The database tier uses MySQL

The application is currently running on a single general purpose large Amazon EC2 instance A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability.

- A. Move static assets to Amazon CloudFront Leave the application in EC2 in an Auto Scaling group Move the database to Amazon RDS to deploy Multi-AZ
- B. Move static assets and the application into a medium EC2 instance Leave the database on one large instance Place both instances in an Auto Scaling group.
- C. Move static assets to Amazon S3 Move the application to AWS Lambda with the concurrency limit set Move the database to Amazon DynamoDB with on-demand enabled.
- D. Move static assets to Amazon S3 Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled Move the database to Amazon RDS to deploy Multi-AZ

Answer(s): D

A company has thousands of edge devices that collectively generate 1 TB of status alerts.

each day Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution However the company needs to minimize costs and does not want to manage additional infrastructure Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements^

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

age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Answer(s): A

An ecommerce company has noticed performance degradation of its Amazon RDS based web application The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer(s): C

A company has an application that ingests incoming messages Dozens of other applications and microservices then quickly consume these messages The number of messages vanes drastically and sometimes increases suddenly to 100 000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics Configure the consumer applications to read and process the messages.
- B. Deploy the ingestion application on Amazon EC2 instances m an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB Configure the consumer applications to read from DynamoDB to process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions Configure the consumer applications to process the messages from the queues.

Answer(s): D

A company provides machine learning solutions .The company's users need to download large data sets from the company's Amazon S3 bucket. These downloads often take a long lime, especially when the users are running many simulations on a subset of those datasets. Users download the datasets to Amazon EC2 instances in the same AWS Region as the S3 bucket. Multiple users typically use the same datasets at the same time. Which solution will reduce the lime that is required to access the datasets?

- A. Configure the S3 bucket lo use the S3 Standard storage class with S3 Transfer Acceleration activated.
- B. Configure the S3 bucket to use the S3 Intelligent-Tiering storage class with S3 Transfer Acceleration activated.
- C. Create an Amazon Elastic File System (Amazon EFS) network Tile system.
Migrate the datasets by using AWS DataSync.
- D. Move the datasets onto a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Attach the volume to all the EC2 instances.

Answer(s): C

A company has three AWS accounts Management Development and Production. These accounts use AWS services only in the us-east-1 Region All accounts have a VPC with VPC Flow Logs configured to publish data to an Amazon S3 bucket in each separate account For compliance reasons the company needs an ongoing method to aggregate all the VPC flow logs across all accounts into one destination S3 bucket in the Management account.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Add S3 Same-Region Replication rules in each S3 bucket that stores VPC flow logs to replicate objects to the destination S3 bucket Configure the destination S3 bucket to allow objects to be received from the S3 buckets in other accounts.
- B. Set up an IAM user in the Management account Grant permissions to the IAM user to access the S3 buckets that contain the VPC flow logs Run the aws s3 sync command in the AWS CLI to copy the objects to the destination S3 bucket.
- C. Use an S3 inventory report to specify which objects in the S3 buckets to copy Perform an S3 batch operation to copy the objects into the destination S3 bucket in the Management account with a single request.
- D. Create an AWS Lambda function in the Management account Grant S3 GET permissions on the source S3 buckets Grant S3 PUT permissions on the destination S3 bucket Configure the function to invoke when objects are loaded in the source S3 buckets.

Answer(s): A

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region Content is made available through an Amazon CloudFront origin pointing to that bucket Cross-Region replication is set up to create a second copy of the bucket in the ap-southeast-1 Region Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Select TWO.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Answer(s): B,E

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access Most of the models are used sporadically but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.

- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Answer(s): D

A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Select TWO)

- A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
- B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
- C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
- D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
- E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

Answer(s): D,E

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling. Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy.

Answer(s): D

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB Me share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Answer(s): D

A company has a website running on Amazon EC2 Instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays and wants to provide a consistent user experience.

How can a solutions architect meet this requirement?

- A. Use step scaling
- B. Use simple scaling
- C. Use lifecycle hooks
- D. Use scheduled scaling

Answer(s): D

A company has multiple AWS accounts for various departments. One of the departments wants to share an Amazon S3 bucket with all other departments. Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket.
- B. Create a pre-signed URL for the bucket and share it with other departments.
- C. Set the S3 bucket policy to allow cross-account access to other departments.
- D. Create IAM users for each of the departments and configure a read-only IAM policy.

Answer(s): C

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

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

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

Answer(s): B

A solution architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Answer(s): A,B

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solutions architect needs to bring that data on-premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center. What should the solutions architect do to meet these requirements?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS) with Lifecycle policies enabled, on AWS. Use it to transfer the data.
- D. Deploy an AWS Snowball device in the on-premises data center after completing an export Job request In the AWS Snowball console.

Answer(s): D

A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.

Which solution will meet these requirements MOST cost-effectively?

- A) Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- B) Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- C) Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
- D) Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Answer(s): C

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows Me system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.

What should a solutions architect do to meet this requirement?

- A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
- B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
- C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Answer(s): B

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user. What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Answer(s): B

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 Bucket A. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Answer(s): D

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS and then relaunch the container.
- B. Create an IAM role with S3 permissions and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3 and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer(s): B

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis.
- D. Amazon ElastiCache for Memcached.

Answer(s): C

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

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-infrequent Access (S3 One Zone-IA)

Answer(s): B

A weather forecasting company needs to process hundreds of gigabytes of data with sub-millisecond latency. The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities.

A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput. Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset.

What should the solutions architect do to meet these requirements?

- A. Use Amazon FSx for Lustre scratch file systems.
- B. Use Amazon FSx for Lustre persistent file systems.
- C. Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode.
- D. Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.

Answer(s): C

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.

What should the solutions architect recommend to build the MOST high-performing solution?**

- A. Use AWS Glue to process data and Amazon S3 to store data.
- B. Use Amazon EMR to process data and Amazon Redshift to store data.
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

Answer(s): A

A company wants to build an immutable infrastructure for its software applications. The company wants to test the software applications before sending traffic to them. The company seeks an efficient solution that limits the effects of application bugs.

Which combination of steps should a solutions architect recommend? {Select TWO}

- A. Use AWS CloudFormation to update the production infrastructure and roll back the stack if the update fails.
- B. Apply Amazon Route 53 weighted routing to test the staging environment and gradually increase the traffic as the tests pass.
- C. Apply Amazon Route 53 failover routing to test the staging environment and fail over to the production environment if the tests pass.
- D. Use AWS CloudFormation with a parameter set to the staging value in a separate environment other than the production environment.
- E. Use AWS CloudFormation to deploy the staging environment with a snapshot deletion policy and reuse the resources in the production environment if the tests pass.

Answer(s): A,E

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.

The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Answer(s): C

A company runs a web-based portal that provides users with global breaking news local alerts, and weather updates. The portal delivers each user a personalized view by using a mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

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

Answer(s): B

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution. What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer(s): A

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running. The business reporting users must be able to generate reports without affecting the application's performance. Which action will accomplish this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Answer(s): D

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

- A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
- D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

Answer(s): A

A security learn needs to enforce the rotation of all IAM users' access keys every 90 days. If an access key is found to be older, the key must be made inactive and removed. A solutions architect must create a solution that will check for and remediate any keys older than 90 days.

Which solution meets these requirements with the LEAST operational effort?

- A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.
- C. Create an AWS Config rule to check for the key age. Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key.

Answer(s): C

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.

What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired trigger instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Answer(s): A

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

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

Answer(s): A

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront: Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Answer(s): D

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

consistent.

Which solution will delete objects that are older than 3 years in the MOST cost-effective manner?

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

Answer(s): B

A solutions architect plans to convert a company's monolithic web application into a multi-tier application. The company wants to avoid managing its own Infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application's API.

Which solution meets these requirements?

- A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
- B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
- C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
- D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

Answer(s): B

A company is deploying an application that processes large quantities of data in batches as needed. The company plans to use Amazon EC2 instances for the workload. The network architecture must support a highly scalable solution and prevent groups of nodes from sharing the same underlying hardware.

Which combination of network solutions will meet these requirements? (Select TWO.)

Create Capacity Reservations for the EC2 instances to run in a placement group.

- A. Run the EC2 instances in a spread placement group.
- B. Run the EC2 instances in a cluster placement group.
- C. Place the EC2 instances in an EC2 Auto Scaling group.
- D. Run the EC2 instances in a partition placement group.

Answer(s): B,C

A company runs a three-tier web application in a VPC across multiple Availability Zones. Amazon EC2 instances run in an Auto Scaling group for the application tier.

The company needs to make an automated scaling plan that will analyze each resource's daily and weekly historical workload trends. The configuration must scale resources appropriately according to both the forecast and live changes in utilization.

Which scaling strategy should a solutions architect recommend to meet these requirements?

- A. Implement dynamic scaling with step scaling based on average CPU utilization from the EC2 instances.
- B. Enable predictive scaling to forecast and scale. Configure dynamic scaling with target tracking.

- C. Create an automated scheduled scaling action based on the traffic patterns of the web application.
- D. Set up a simple scaling policy Increase the cool down period based on the EC2 instance start up time.

Answer(s): B

A company maintains about 300 TB in Amazon S3 Standard storage month after month. The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application. The number and size of S3 objects remain constant but the company's S3 storage costs are increasing each month.

How should a solutions architect reduce costs in this situation?

- A. Switch from multipart uploads to Amazon S3 Transfer Acceleration.
- B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads.
- C. Configure S3 inventory to prevent objects from being archived too quickly.
- D. Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3

Answer(s): B

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Answer(s): B

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.

Which networking solution meets these requirements?

- A. Place the EC2 instances in multiple VPCs and configure VPC peering.
- B. Attach an Elastic Fabric Adapter (EFA) to each EC2 instance.
- C. Run the EC2 instances in a spread placement group.
- D. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Answer(s): B

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront

distribution A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer(s): B

An application uses an Amazon RDS MySQL DB instance The RDS database is becoming low on disk space A solutions architect wants to increase the disk space without downtime Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage autoscaling in RDS
- B. Increase the RDS database instance size.
- C. Change the RDS database instance storage type to Provisioned IOPS
- D. Back up the RDS database increase the storage capacity restore the database and stop the previous instance.

Answer(s): A

A solutions architect is creating an application that will handle batch processing of large amounts of data The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

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

Answer(s): C

A company wants to enforce strict security guidelines on accessing AWS Cloud resources as the company migrates production workloads from its data centers. Company management wants all users to receive permissions according to their job roles and functions.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an AWS Single Sign-On deployment. Connect to the on-premises Active Directory to centrally manage users and permissions across the company.
- B. Create an IAM role for each job function. Require each employee to call the stsAssumeRole action in the AWS Management Console to perform their job role.
- C. Create individual IAM user accounts for each employee Create an IAM policy for each job function, and attach the policy to all IAM users based on their job role.

- D. Create individual IAM user accounts for each employee. Create IAM policies for each job function. Create IAM groups, and attach associated policies to each group. Assign the IAM users to a group based on their Job role.

Answer(s): D

A company has designed an application where users provide small sets of textual data by calling a public API. The application runs on AWS and includes a public Amazon API Gateway API that forwards requests to an AWS Lambda function for processing. The Lambda function then writes the data to an Amazon Aurora Serverless database for consumption.

The company is concerned that it could lose some user data if a Lambda function fails to process the request properly or reaches a concurrency limit.

What should a solutions architect recommend to resolve this concern?

- A. Split the existing Lambda function into two Lambda functions. Configure one function to receive API Gateway requests and put relevant items into Amazon Simple Queue Service (Amazon SQS). Configure the other function to read items from Amazon SQS and save the data into Aurora.
- B. Configure the Lambda function to receive API Gateway requests and write relevant items to Amazon ElastiCache. Configure ElastiCache to save the data into Aurora.
- C. Increase the memory for the Lambda function. Configure Aurora to use the Multi-AZ feature.
- D. Split the existing Lambda function into two Lambda functions. Configure one function to receive API Gateway requests and put relevant items into Amazon Simple Notification Service (Amazon SNS). Configure the other function to read items from Amazon SNS and save the data into Aurora.

Answer(s): A

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer(s): A

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before securing it to Amazon S3.

What should a solutions architect recommend to safely meet these requirements?

- A. Server-side encryption with customer-provided encryption keys.
- B. Client-side encryption with Amazon S3 managed encryption keys.
- C. Service-side encryption with keys stored in AWS Management Service (AWS KMS)
- D. Server-side encryption with a master stored in AWS Management Service (AWS KMS)

Answer(s): D

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business To ensure this does not happen again the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer(s): B

A startup company is using the AWS Cloud to develop a traffic control monitoring system for a large city. The system must be highly available and must provide near-real-time results for residents and city officials even during peak events.

Gigabytes of data will come in daily from IoT devices that run at intersections and freeway ramps across the city. The system must process the data sequentially to provide the correct timeline. However results need to show only what has happened in the last 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon Kinesis Data Firehose to accept incoming data from the IoT devices and write the data to Amazon S3. Build a web dashboard to display the data from the last 24 hours.
- B. Deploy an Amazon API Gateway API endpoint and an AWS Lambda function to process incoming data from the IoT devices and store the data in Amazon DynamoDB. Build a web dashboard to display the data from the last 24 hours.
- C. Deploy an Amazon API Gateway API endpoint and an Amazon Simple Notification Service (Amazon SNS) topic to process incoming data from the IoT devices. Write the data to Amazon Redshift. Build a web dashboard to display the data from the last 24 hours.
- D. Deploy an Amazon Simple Queue Service (Amazon SQS) FIFO queue and an AWS Lambda function to process incoming data from the IoT devices and store the data in an Amazon RDS DB instance. Build a web dashboard to display the data from the last 24 hours.

Answer(s): D

A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the Internet, and a

VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch.

Which solution meets these requirements?

- A. Use two ALBs: one for on premises and one for the AWS resource Add hosts to each target group of each ALB Route with Amazon Route 53 based on the URL query string.
- B. Use one ALB; one for on premises and one for the AWS resource Add hosts to the target group of each ALB Create a software router on an EC2 instance based on the URL query string.
- C. Use one ALB with two target groups one for the AWS resource and one for on premises Add hosts to each target group of the ALB Configure listener rules based on the URL query string.
- D. Use one ALB with two AWS Auto Scaling groups one for the AWS resource and one for on premises Add hosts to each Auto Scaling group Route with Amazon Route 53 based on the URL query string.

Answer(s): C

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Answer(s): A

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Conned connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Conned connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Conned connection at a location in the same Region.

Answer(s): D

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists. The company is looking for a native, software-based AWS service to accomplish this goal.

What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Answer(s): A

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.

What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
- B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory on the current EC2 instance.
- C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active Directory domain controller running on the current EC2 instance.
- D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer(s): A

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the OynamoDB table continuously grows but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.

Which solution meets these requirements?

- A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the Cloud Formation stack every 30 days, and delete the original stack.
- B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
- C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
- D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Answer(s): D

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Answer(s): D

A developer has a script to generate daily reports that users previously ran manually. The script consistently completes in under 10 minutes. The developer needs to automate this process in a cost-effective manner.

Which combination of services should the developer use? (Select TWO.)

- A. AWS Lambda
- B. AWS CloudTrail
- C. Cron on an Amazon EC2 instance
- D. Amazon EC2 On-Demand Instance with user data
- E. Amazon EventBridge (Amazon CloudWatch Events)

Answer(s): A,E

A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
- B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
- C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
- D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Answer(s): A

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data. The solution must be fully managed.

Which AWS solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system Mount the file system to the application server.
- B. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance Connect the application server to the file share.
- C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server Connect the application server to the file system.
- D. Create an Amazon S3 bucket Assign an IAM role to the application to grant access to the S3 bucket Mount the S3 bucket to the application server.

Answer(s): C

A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

- A. Amazon Redshift.
- B. AWS Storage Gateway for files.
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Answer(s): B

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture.

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.
- B. Use Amazon CloudWatch Logs to store the logs Run SQL queries as needed from the Amazon CloudWatch console.
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.
- D. Use AWS Glue to catalog the logs Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

Answer(s): C

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.

How should a solutions architect optimize high availability for the application?

- A. Use lambda@Edge for CloudFront.
- B. Use Amazon S3 Transfer Acceleration for CloudFront.
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Answer(s): A

A company is migrating Us applications to AWS Currently applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system The company Is running an analytics application in the cloud that runs hourly to generate Insights from this data.

The company needs a solution to handle the ongoing data transfer between the on- premises shared file system and Amazon S3 The solution also must be able to handle occasional interruptions m internet connectivity.

Which solution should the company use for the data transfer to meet these requirements?

- A. AWS DataSync
- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

Answer(s): A

A solutions architect is designing the storage architecture tor a new web application used for storing and viewing engineering drawings All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load The application must be able to store petabytes of data.

Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon BBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Answer(s): A

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images Image customization parameters wilt be in every request that is sent to an Amazon API Gateway API. The solution will generate tie customized images on demand. Users will receive a link that they can use to view or download their customized images. The solution must be highly available for viewing and customizing images.

What should the solutions architect do to meet these requirements MOST cost effectively?

- A. Use Amazon EC2 instances to manipulate the original images into the requested customizations Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front. of the EC2 Instances.
- B. Use AWS Lambda to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original images into the requested customizations Store the original images in Amazon S3 Store the manipulated images in Amazon DynamoDB. Provision an Application Load Balancer and Amazon EC2 instances to serve the content.
- D. Use Amazon EC2 instances to manipulate the original Images Into the requested customizations. Store the original images in Amazon S3. Store the manipulated Images m Amazon DynamoDB Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer(s): B

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
- D. Configure Amazon Route S3 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

Answer(s): A

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.

How should the company write its application to handle these database requests?

- A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
- B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Answer(s): D

A company is running a multi-tier recommendation web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance degrades when the number of read and write IOPS is higher than 20,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a magnetic volume.
- B. Increase the number of IOPS on the gp3 volume.
- C. Replace the volume with a Provisioned IOPS SSD (Io2) volume.
- D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

Answer(s): C

A company develops web applications. As part of its development process, the company constantly launches and deletes Application Load Balancers (ALBs) in multiple AWS Regions.

The company wants to create an allow list on its firewall device. The allow list will contain the IP addresses of all the load balancers. A solutions architect needs a one-line, highly available solution that will accomplish that goal and will help reduce the number of IP addresses that the firewall needs to allow.

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

- A. Create an AWS Lambda function to keep track of the IP addressee for all the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IP addresses Register the private IP addresses of all the ALBs as targets for the NLB
- C. Launch AWS Global Accelerator Create endpoints for each of the Regions that are in use. Register all the ALBs in the Regions to the corresponding endpoints.
- D. Set up an Amazon EC2 Instance Assign an Elastic IP address to the EC2 instance. Configure the EC2 instance as a proxy to forward traffic to all the ALBs.

Answer(s): C

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

What should a solutions architect do to meet these requirement with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Answer(s): C

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile D Store AWS access key directly on the EC2 instance for applications on the instance to use for API calls.

Answer(s): C

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

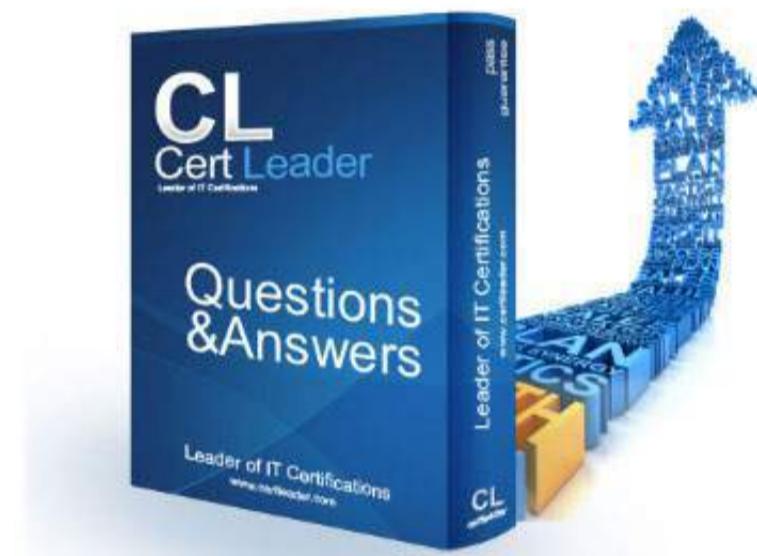
- A. AW3 Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Answer(s): B

SAA-C02 Dumps

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.certleader.com/SAA-C02-dumps.html>



NEW QUESTION 1

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO.)

- A. Configure a VPC peering connection between the two VPC
- B. Access the API using the private address
- C. Configure an AWS Direct Connect connection between the two VPC
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VP
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts Access the API using the private address

Answer: DE

NEW QUESTION 2

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company. How should security groups be configured in this situation? (Select TWO.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

Answer: AC

NEW QUESTION 3

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB). Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Answer: B

NEW QUESTION 4

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective. What should a solutions architect do to meet these requirements? (Select TWO.)

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Answer: CE

NEW QUESTION 5

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application. Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier

Answer: B

NEW QUESTION 6

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm. Which service should the solutions architect use?

- A. Amazon EFS

- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Answer: B

NEW QUESTION 7

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 8

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be stored in multiple AWS Regions. How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

NEW QUESTION 9

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained. What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

NEW QUESTION 10

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Answer: D

NEW QUESTION 10

A company has an application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications. Which action will fulfill these requirements and maintain security?

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

Answer: C

NEW QUESTION 11

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: C

NEW QUESTION 15

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C

NEW QUESTION 18

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.

What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the applicatio
- E. Enforce multifactor authentication.

Answer: C

NEW QUESTION 22

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C**NEW QUESTION 23**

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images. What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B**NEW QUESTION 26**

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Answer: C**NEW QUESTION 27**

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently. How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket.
- B. Use S3 event notifications to invoke microservice 2.
- C. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- D. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose.
- E. Implement code in microservice 2 to read from Kinesis Data Firehose.
- F. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Answer: C**NEW QUESTION 31**

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C**NEW QUESTION 33**

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket. Which action will MOST securely grant the EC2 instance access to the S3 bucket?

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile.

D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls

Answer: C

NEW QUESTION 34

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 37

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States. Which changes should be made to the database tier to improve performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
- C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Answer: D

NEW QUESTION 38

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 39

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Answer: D

NEW QUESTION 44

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity.
- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance.
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 46

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID
- B. Store the password in AWS Secrets Manager Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID
- C. Move the database password to an environment variable associated with the Lambda function Retrieve the password from the environment variable upon execution
- D. Store the password in AWS Key Management Service (AWS KMS) Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID

Answer: B

NEW QUESTION 51

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months. Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume Mount the EBS volume on the application instances
- B. Store the data in an Amazon EFS file system Mount the file system on the application instances
- C. Store the data in Amazon S3 Glacier Update the vault policy to allow access to the application instances
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) Update the bucket policy to allow access to the application instances

Answer: B

NEW QUESTION 52

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS
- B. Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- C. Use AWS Storage Gateway to move existing data to AWS Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS DataSync to move existing data to AWS Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- E. Use AWS Storage Gateway to move existing data to AWS Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data Enable Amazon S3 object lock and enable Amazon S3 server access logging

Answer: B

NEW QUESTION 54

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on-premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD

NEW QUESTION 58

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

NEW QUESTION 62

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

100% Pass Your SAA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAA-C02-dumps.html>

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.2passeeasy.com/dumps/SAA-C02/>



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

static website within an Amazon S3 bucket. A solutions architect needs to accomplish this?

- A. Enable Amazon S3 versioning.
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy.
- D. Enable Amazon S3 cross-Region replication.

Answer: A

NEW QUESTION 3

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.

Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register the instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Answer: A

NEW QUESTION 4

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

NEW QUESTION 5

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 6

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time. Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.

D. Purchase Reserved Instances to cover 50 instances Use On-Demand and Spot Instances to cover the remaining instances

Answer: D

NEW QUESTION 7

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.

There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi.AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Answer: D

NEW QUESTION 8

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 9

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C

NEW QUESTION 10

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID). What should a solutions architect do to meet these requirements?

- A. Launch the application on EC2 instances in each Availability Zone
- B. Attach EBS volumes to each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- E. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: C

NEW QUESTION 10

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy.
- E. Create alias records in Route 53 that point to the Application Load Balancer.

Answer: B

NEW QUESTION 14

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time. What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application.
- E. Enforce multifactor authentication.

Answer: C

NEW QUESTION 19

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 22

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images. What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B

NEW QUESTION 25

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Answer: C

NEW QUESTION 29

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Explanation:

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

NEW QUESTION 34

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Answer: A

NEW QUESTION 39

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 42

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 43

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer Put the web layer behind the load balancer and enable AWS WAF
- B. Create a Network Load Balancer Put the web layer behind the load balancer and enable AWS WAF
- C. Create an Application Load Balancer Put the web layer behind the load balancer and enable AWS WAF
- D. Create an Application Load Balancer Put the web layer behind the load balancer and use AWS Shield Standard

Answer: C

NEW QUESTION 45

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

Answer: C

NEW QUESTION 48

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue
- B. Use the AddPermission API call to add appropriate permissions
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Answer: D

NEW QUESTION 52

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity

- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance.
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replica.
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 57

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory.
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connecto.
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory contolle.
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 59

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups. What should be done to enable encryption for future backups?"

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database Copy it to an encrypted snapshot Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL Promote the encrypted read replica to primary Remove the original database instance.

Answer: C

NEW QUESTION 62

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer. After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?"

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Answer: C

NEW QUESTION 65

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 69

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS) Associate the Lambda function with a role that can retrieve the password from AWS KMS.

given its key ID

Answer: B

NEW QUESTION 74

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 78

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

NEW QUESTION 82

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Answer: B

NEW QUESTION 85

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAA-C02 Product From:

<https://www.2passeeasy.com/dumps/SAA-C02/>

Money Back Guarantee

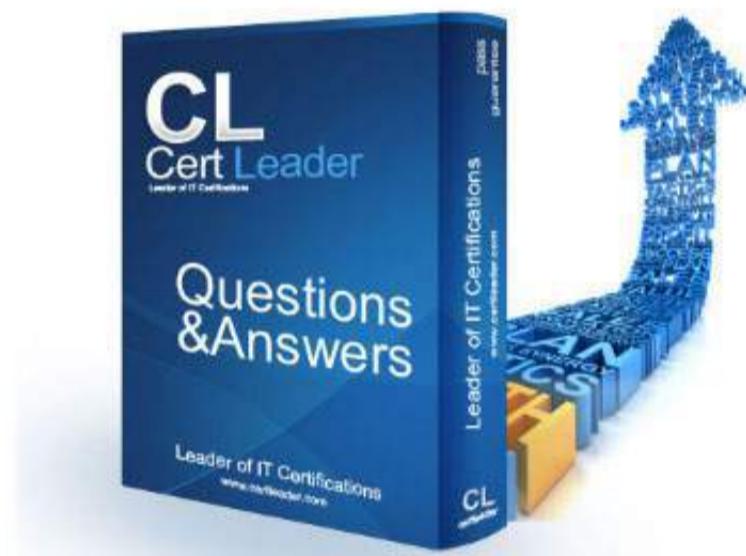
SAA-C02 Practice Exam Features:

- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

SAA-C02 Dumps

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.certleader.com/SAA-C02-dumps.html>



NEW QUESTION 1

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective. What should a solutions architect do to meet these requirements? (Select TWO.)

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Answer: CE

NEW QUESTION 2

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

NEW QUESTION 3

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 4

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Answer: D

NEW QUESTION 5

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.

There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi.AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Answer: D

NEW QUESTION 6

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Answer: B**NEW QUESTION 7**

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow. Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

Answer: A**NEW QUESTION 8**

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C**NEW QUESTION 9**

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database. What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database
- B. Update the application to read from the Multi-AZ standby instance
- C. Create a read replica and modify the application to use the appropriate endpoint
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C**NEW QUESTION 10**

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID). What should a solutions architect do to meet these requirements?

- A. Launch the application on EC2 instances in each Availability Zone
- B. Attach EBS volumes to each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- E. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: C**NEW QUESTION 10**

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group
- B. Use a target tracking policy to dynamically scale the Auto Scaling group
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: D**NEW QUESTION 14**

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: C

NEW QUESTION 17

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application. How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica

Answer: B

NEW QUESTION 18

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time. What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the applicatio
- E. Enforce multifactor authentication.

Answer: C

NEW QUESTION 20

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images. What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

C. Use AWS Lambda to manipulate the original image to the requested customization Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB Configure an Elastic Load Balancer in front of the Amazon EC2 instances

D. Use Amazon EC2 instances to manipulate the original image into the requested customization Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB Configure an Amazon CloudFront distribution with the S3 bucket as the origin

Answer: B

NEW QUESTION 22

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access

Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI) Configure the distribution with an Amazon S3 origin to provide access to the file through signed URL's Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file Design the application to track purchases in a DynamoDB tableConfigure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB
- C. Use an Amazon CloudFront distribution with an OAI Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs Design the application to set an expiration of 14 days for the URL
- D. Use an Amazon CloudFront distribution with an OAI Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary

Answer: C

NEW QUESTION 23

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket
- B. Use S3 event notifications to invoke microservice 2.
- C. Implement code in microservice 1 to publish data to an Amazon SNS topic Implement code in microservice 2 to subscribe to this topic
- D. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose
- E. Implement code in microservice 2 to read from Kinesis Data Firehose.
- F. Implement code in microservice 1 to send data to an Amazon SQS queue Implement code in microservice 2 to process messages from the queue

Answer: C

NEW QUESTION 28

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

NEW QUESTION 33

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 35

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meets these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 40

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

- A. Create new public and private subnets in the same AZ for high availability
 - B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs
 - C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer
 - D. Create new public and private subnets in a new AZ
 - E. Create new public and private subnets in the same VPC each in a new AZ
- Migrate the database to an Amazon RDS multi-AZ deployment

Answer: BE

NEW QUESTION 45

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity
- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 48

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connector
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 49

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups. What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance

Answer: C

NEW QUESTION 50

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents. Which combination of actions should be taken to meet these requirements? (Select TWO.)

- A. Enable a read-only bucket ACL
- B. Enable versioning on the bucket
- C. Attach an IAM policy to the bucket
- D. Enable MFA Delete on the bucket
- E. Encrypt the bucket using AWS KMS

Answer: BD

NEW QUESTION 54

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures. What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB

- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked
D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

Answer: B

NEW QUESTION 57

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 61

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 62

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance. Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS

Answer: B

NEW QUESTION 66

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates. Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.
- B. Add Aurora Replicas
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 70

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?"

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

Answer: D

NEW QUESTION 74

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and

support future records

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AW
- B. Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- C. Use AWS Storage Gateway to move existing data to AWS Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS DataSync to move existing data to AWS Use Amazon S3 to store existing and new data Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- E. Use AWS Storage Gateway to move existing data to AWS Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data Enable Amazon S3 object lock and enable Amazon S3 server access logging

Answer: B

NEW QUESTION 78

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD

NEW QUESTION 81

A company allows its developers to attach existing IAM policies to existing IAM roles to enable (aster experimentation and agility However the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 84

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet What should the solutions architect do to accomplish this? (Select TWO)

- A. Create a route table entry for the endpoint
- B. Create a gateway endpoint for DynamoDB
- C. Create a new DynamoDB table that uses the endpoint
- D. Create an ENI for the endpoint in each of the subnets of the VPC
- E. Create a security group entry in the default security group to provide access

Answer: AB

NEW QUESTION 85

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

100% Pass Your SAA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAA-C02-dumps.html>

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.2passeeasy.com/dumps/SAA-C02/>



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year. Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

NEW QUESTION 3

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO)

- A. Configure a VPC peering connection between the two VPCs.
- B. Access the API using the private address.
- C. Configure an AWS Direct Connect connection between the two VPCs.
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VPC.
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Answer: DE

NEW QUESTION 4

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are auto scaling EC2_INSTANCE_LAUNCH events.

Answer: B

NEW QUESTION 5

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company. How should security groups be configured in this situation? (Select TWO)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Answer: AC

NEW QUESTION 6

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 7

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience. Which service will improve the performance of both the real-time and on-demand streaming?

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

Answer: A

NEW QUESTION 8

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys. What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: C

NEW QUESTION 9

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be stored in multiple AWS Regions. How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

NEW QUESTION 10

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained. What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

NEW QUESTION 10

A company has an application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications. Which action will fulfill these requirements and maintain security?

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

Answer: C

NEW QUESTION 11

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs. Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C

NEW QUESTION 14

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 16

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Answer: AB

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

NEW QUESTION 21

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Explanation:

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

NEW QUESTION 25

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer: B

NEW QUESTION 27

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Answer: A

NEW QUESTION 31

A company's application is running on Amazon EC2 instances in a single Region in the event of a disaster a solutions architect needs to ensure that the resources can also be deployed to a second Region

Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3
- B. Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

NEW QUESTION 33

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

NEW QUESTION 37

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files
- B. Use cross-Region replication to all Regions
- C. Use the geoproximity feature of Amazon Route 53
- D. Use Amazon CloudFront with the S3 bucket as its origin

Answer: D

NEW QUESTION 41

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity.
- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance.
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 45

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Answer: B

NEW QUESTION 47

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Answer: C

NEW QUESTION 49

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 53

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Answer: B

NEW QUESTION 56

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Answer: B

NEW QUESTION 60

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Answer: AB

NEW QUESTION 65

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAA-C02 Product From:

<https://www.2passeeasy.com/dumps/SAA-C02/>

Money Back Guarantee

SAA-C02 Practice Exam Features:

- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

Amazon-Web-Services

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year. Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

NEW QUESTION 3

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO)

- A. Configure a VPC peering connection between the two VPCs.
- B. Access the API using the private address.
- C. Configure an AWS Direct Connect connection between the two VPCs.
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VPC.
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Answer: DE

NEW QUESTION 4

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

NEW QUESTION 5

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 6

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier

Answer: B

NEW QUESTION 7

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time. Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances
- B. Purchase Reserved Instances to cover 80 instances Use Spot Instances to cover the remaining instances
- C. Purchase On-Demand Instances to cover 40 instances Use Spot Instances to cover the remaining instances
- D. Purchase Reserved Instances to cover 50 instances Use On-Demand and Spot Instances to cover the remaining instances

Answer: D

NEW QUESTION 8

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow. Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

Answer: A

NEW QUESTION 9

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 10

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be stored in multiple AWS Regions. How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

NEW QUESTION 10

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput. Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone
- B. Launch the EC2 instances in a spread placement group in one Availability Zone
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A

NEW QUESTION 11

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group
- B. Use a target tracking policy to dynamically scale the Auto Scaling group

- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: D

NEW QUESTION 15

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: B

NEW QUESTION 19

A company has applications running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

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

Answer: C

NEW QUESTION 20

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: C

NEW QUESTION 22

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a

new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application. How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Answer: B

NEW QUESTION 23

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability. What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy.
- E. Create alias records in Route 53 that point to the Application Load Balancer.

Answer: B

NEW QUESTION 25

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 27

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Answer: AB

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

NEW QUESTION 28

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Explanation:

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

NEW QUESTION 32

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently. How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket.
- B. Use S3 event notifications to invoke microservice 2.

- C. Implement code in microservice 1 to publish data to an Amazon SNS topic Implement code in microservice 2 to subscribe to this topic
- D. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose
- E. Implement code in microservice 2 to read from Kinesis Data Firehose.
- F. Implement code in microservice 1 to send data to an Amazon SQS queue Implement code in microservice 2 to process messages from the queue

Answer: C

NEW QUESTION 34

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C

NEW QUESTION 36

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer: B

NEW QUESTION 37

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

NEW QUESTION 41

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 43

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States. Which changes should be made to the database tier to improve performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
- C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Answer: D

NEW QUESTION 47

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing. Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon EBS Provisioned IOPS SSD (io1)

Answer: B

NEW QUESTION 49

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication. Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 52

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume. Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 54

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ). Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

- A. Create new public and private subnets in the same AZ for high availability
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ
- E. Create new public and private subnets in the same VPC each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Answer: BE

NEW QUESTION 56

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution. Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files
- B. Use cross-Region replication to all Regions
- C. Use the geoproximity feature of Amazon Route 53
- D. Use Amazon CloudFront with the S3 bucket as its origin

Answer: D

NEW QUESTION 57

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue
- B. Use the AddPermission API call to add appropriate permissions
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Answer: D

NEW QUESTION 58

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity.
- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance.
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 62

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory.
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connecto
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory contolle
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 64

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months. Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume Mount the EBS volume on the application instances
- B. Store the data in an Amazon EFS file system Mount the file system on the application instances
- C. Store the data in Amazon S3 Glacier Update the vault policy to allow access to the application instances
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) Update the bucket policy to allow access to the application instances

Answer: B

NEW QUESTION 65

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 68

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance. Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS

Answer: B

NEW QUESTION 73

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates. Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.
- B. Add Aurora Replicas

- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 78

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 81

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SAA-C02 Practice Exam Features:

- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SAA-C02 Practice Test Here](#)



Amazon-Web-Services

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)

NEW QUESTION 1

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 2

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Answer: D

NEW QUESTION 3

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 4

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: C

NEW QUESTION 5

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

NEW QUESTION 6

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database
- B. Update the application to read from the Multi-AZ standby instance
- C. Create a read replica and modify the application to use the appropriate endpoint
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C

NEW QUESTION 7

An Amazon EC2 administrator created the following policy associated with an 1AM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: C

NEW QUESTION 8

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

NEW QUESTION 9

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C

NEW QUESTION 10

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 10

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B

NEW QUESTION 13

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication. Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 15

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Answer: D

NEW QUESTION 18

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Select TWO)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer: BC

NEW QUESTION 21

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory.
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connecto
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory contolle
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 23

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores

user-uploaded documents in an Amazon EBS volume. For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer. After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?"

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

Answer: C

NEW QUESTION 26

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 29

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

NEW QUESTION 30

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 35

.....

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

NEW QUESTION 2

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Answer: D

NEW QUESTION 3

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 4

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: C

NEW QUESTION 5

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

NEW QUESTION 6

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database
- B. Update the application to read from the Multi-AZ standby instance
- C. Create a read replica and modify the application to use the appropriate endpoint
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C

NEW QUESTION 7

An Amazon EC2 administrator created the following policy associated with an 1AM group containing several users.

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.1001 in the us-east-1 Region
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254

Answer: C

NEW QUESTION 8

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

NEW QUESTION 9

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C

NEW QUESTION 10

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 10

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B

NEW QUESTION 13

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication. Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 15

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Answer: D

NEW QUESTION 18

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Select TWO)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer: BC

NEW QUESTION 21

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory.
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connecto
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory contolle
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 23

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores

user-uploaded documents in an Amazon EBS volume. For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer. After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?"

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

Answer: C

NEW QUESTION 26

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 29

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

NEW QUESTION 30

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 35

.....

Relate Links

100% Pass Your SAA-C02 Exam with Exambible Prep Materials

<https://www.exambible.com/SAA-C02-exam/>

Contact us

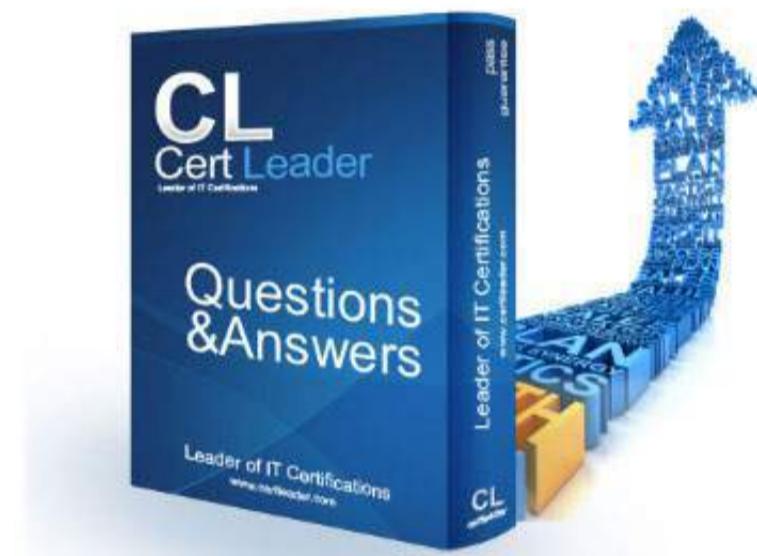
We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>

SAA-C02 Dumps

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.certleader.com/SAA-C02-dumps.html>



NEW QUESTION 1

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO)

- A. Configure a VPC peering connection between the two VPC
- B. Access the API using the private address
- C. Configure an AWS Direct Connect connection between the two VPC
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VP
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts Access the API using the private address

Answer: DE

NEW QUESTION 2

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%. which disrupts the application. What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

Answer: C

NEW QUESTION 3

static website within an Amazon S3 bucket. A solutions architect needs to Which action will accomplish this?

- A. Enable Amazon S3 versioning
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy
- D. Enable Amazon S3 cross-Region replication.

Answer: A

NEW QUESTION 4

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm. Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Answer: B

NEW QUESTION 5

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 6

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained. What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions

Answer: D

NEW QUESTION 7

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput. Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone
- B. Launch the EC2 instances in a spread placement group in one Availability Zone
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A

NEW QUESTION 8

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO.)

- A. Ensure the root user uses a strong password
- B. Enable multi-factor authentication to the root user
- C. Store root user access keys in an encrypted Amazon S3 bucket
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document

Answer: AB

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

NEW QUESTION 9

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Answer: C

NEW QUESTION 10

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C

NEW QUESTION 10

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website. What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Answer: A

NEW QUESTION 11

A company's application is running on Amazon EC2 instances in a single Region in the event of a disaster a solutions architect needs to ensure that the resources can also be deployed to a second Region
Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3
- B. Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

NEW QUESTION 15

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 18

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 23

A company has a three-tier image-sharing application it uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Answer: D

NEW QUESTION 28

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

- A. Create new public and private subnets in the same AZ for high availability
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ
- E. Create new public and private subnets in the same VPC each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Answer: BE

NEW QUESTION 33

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Select TWO.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB

- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer: BC

NEW QUESTION 35

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue
- B. Use the AddPermission API call to add appropriate permissions
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout

Answer: D

NEW QUESTION 40

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups. What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance

Answer: C

NEW QUESTION 42

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures. What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

Answer: B

NEW QUESTION 46

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 51

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

100% Pass Your SAA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAA-C02-dumps.html>

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.2passeeasy.com/dumps/SAA-C02/>



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application. What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Answer: C

NEW QUESTION 3

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution. What should a solutions architect do to accomplish this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
- D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Answer: B

NEW QUESTION 4

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow. Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register the instances with the same ALB using cross-Region VPC peering.
- E. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Answer: A

NEW QUESTION 5

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application. Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

NEW QUESTION 6

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience. Which service will improve the performance of both the real-time and on-demand streaming?

- A. Amazon CloudFront
- B. AWS Global Accelerator

- C. Amazon Route 53
D. Amazon S3 Transfer Acceleration

Answer: A

NEW QUESTION 7

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time. Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances
- B. Purchase Reserved Instances to cover 80 instances Use Spot Instances to cover the remaining instances
- C. Purchase On-Demand Instances to cover 40 instances Use Spot Instances to cover the remaining instances
- D. Purchase Reserved Instances to cover 50 instances Use On-Demand and Spot Instances to cover the remaining instances

Answer: D

NEW QUESTION 8

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm. Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Answer: B

NEW QUESTION 9

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow. Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

Answer: A

NEW QUESTION 10

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries. Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C

NEW QUESTION 10

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be stored in multiple AWS Regions. How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

NEW QUESTION 14

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput. Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone
- B. Launch the EC2 instances in a spread placement group in one Availability Zone
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A

NEW QUESTION 17

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month. Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: B

NEW QUESTION 22

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

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

Answer: C

NEW QUESTION 26

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

NEW QUESTION 31

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Explanation:

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

NEW QUESTION 36

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B

NEW QUESTION 40

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination

E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

NEW QUESTION 44

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing. Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon EBS Provisioned IOPS SSD (io1)

Answer: B

NEW QUESTION 49

A company has a two-tier application architecture that runs in public and private subnets Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ). Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

- A. Create new public and private subnets in the same AZ for high availability
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer
- D. Create new public and private subnets in a new AZ Create a database using Amazon EC2 in one AZ
- E. Create new public and private subnets in the same VPC each in a new AZ Migrate the database to an Amazon RDS multi-AZ deployment

Answer: BE

NEW QUESTION 50

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

Answer: C

NEW QUESTION 53

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 57

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months. Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Answer: B

NEW QUESTION 62

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

- A. Add AWS Shield.
- B. Add Aurora Replicas
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.

E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 66

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instances. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

NEW QUESTION 68

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO)

- A. Create a route table entry for the endpoint
- B. Create a gateway endpoint for DynamoDB
- C. Create a new DynamoDB table that uses the endpoint
- D. Create an ENI for the endpoint in each of the subnets of the VPC
- E. Create a security group entry in the default security group to provide access

Answer: AB

NEW QUESTION 72

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAA-C02 Product From:

<https://www.2passeeasy.com/dumps/SAA-C02/>

Money Back Guarantee

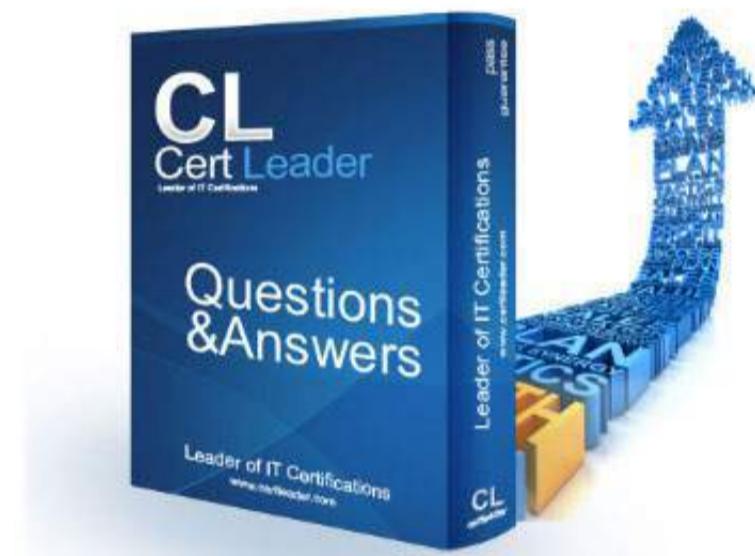
SAA-C02 Practice Exam Features:

- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

SAA-C02 Dumps

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.certleader.com/SAA-C02-dumps.html>



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year. Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

NEW QUESTION 3

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO)

- A. Configure a VPC peering connection between the two VPC
- B. Access the API using the private address
- C. Configure an AWS Direct Connect connection between the two VPC
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VP
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts Access the API using the private address

Answer: DE

NEW QUESTION 4

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are auto scaling EC2_INSTANCE_LAUNCH events

Answer: B

NEW QUESTION 5

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution. What should a solutions architect do to accomplish this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
- D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Answer: B

NEW QUESTION 6

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow. Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin Then update the Amazon Route 53 record to point to the CloudFront distribution
- B. Create a latency-based Amazon Route 53 record for the ALB Then launch new EC2 instances with larger instance sizes and register the instances with the ALB
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register the instances with the same ALB using cross-Region VPC peering
- E. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances Then update an Amazon Route 53 record to point to the S3 buckets

Answer: A

NEW QUESTION 7

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3

Answer: A

NEW QUESTION 8

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage.

There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi.AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Answer: D

NEW QUESTION 9

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow. Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

Answer: A

NEW QUESTION 10

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 10

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C

NEW QUESTION 14

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID). What should a solutions architect do to meet these requirements?

- A. Launch the application on EC2 instances in each Availability Zone
- B. Attach EBS volumes to each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones Mount an instance store on each EC2 instance
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- E. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: C

NEW QUESTION 17

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

NEW QUESTION 21

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application. How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance
- C. Create multiple RDS Read Replicas of the production RDS DB instance Place the Read Replicas in an Auto Scaling group
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance Create a second Single-AZ RDS Read Replica from the replica

Answer: B

NEW QUESTION 23

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs. Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C

NEW QUESTION 24

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time. What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the applicatio
- E. Enforce multifactor authentication.

Answer: C

NEW QUESTION 25

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled Move all the data to Amazon S3 Delete the RDS instance
- B. Enable RDS Multi-AZ mode with encryption at rest enabled Perform a failover to the standby instance to delete the original instance
- C. Take a snapshot of the RDS instance Create an encrypted copy of the snapshot Restore the RDS instance from the encrypted snapshot
- D. Create an RDS read replica with encryption at rest enabled Promote the read replica to master and switch the application over to the new master Delete the old RDS instance.

Answer: C

NEW QUESTION 29

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Answer: B

NEW QUESTION 32

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

NEW QUESTION 34

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 36

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

NEW QUESTION 41

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 44

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Answer: C

NEW QUESTION 49

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that

allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

Answer: C

NEW QUESTION 54

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours. Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity.
- B. Refactor the application to use DynamoDB for reports.
- C. Create the database on a compute optimized Amazon EC2 instance.
- D. Ensure compute resources exceed the on-premises database.
- E. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas.
- F. Configure the application reader endpoint for reports.
- G. Create an Amazon Aurora MySQL Multi-AZ DB cluster.
- H. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: B

NEW QUESTION 59

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff. What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory.
- B. Uninstall Active Directory on the current EC2 instance.
- C. Create another EC2 instance in the same subnet and reinstall Active Directory on it.
- D. Uninstall Active Directory.
- E. Use AWS Directory Service to create an Active Directory connector.
- F. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- G. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller.
- H. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: C

NEW QUESTION 61

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Answer: C

NEW QUESTION 66

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage.

The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Select TWO.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Answer: BD

NEW QUESTION 69

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures. What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin.

- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

Answer: B

NEW QUESTION 70

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Answer: B

NEW QUESTION 72

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Answer: B

NEW QUESTION 73

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 75

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

- A. Add AWS Shield.
- B. Add Aurora Replicas.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Answer: DE

NEW QUESTION 77

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on a separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

NEW QUESTION 80

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning. How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Answer: B**NEW QUESTION 82**

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Answer: D**Explanation:**

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 83

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Answer: AB**NEW QUESTION 84**

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

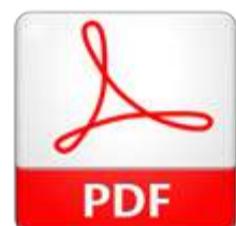
100% Pass Your SAA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAA-C02-dumps.html>

Amazon-Web-Services

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)



NEW QUESTION 1

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

NEW QUESTION 2

static website within an Amazon S3 bucket. A solutions architect needs to accomplish this?

- A. Enable Amazon S3 versioning
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy
- D. Enable Amazon S3 cross-Region replication.

Answer: A

NEW QUESTION 3

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Select TWO.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

Answer: AC

NEW QUESTION 4

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Answer: B

NEW QUESTION 5

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.

What should a solutions architect do to meet these requirements? (Select TWO.)

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Answer: CE

NEW QUESTION 6

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

NEW QUESTION 7

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time. Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances
- B. Purchase Reserved Instances to cover 80 instances Use Spot Instances to cover the remaining instances
- C. Purchase On-Demand Instances to cover 40 instances Use Spot Instances to cover the remaining instances
- D. Purchase Reserved Instances to cover 50 instances Use On-Demand and Spot Instances to cover the remaining instances

Answer: D

NEW QUESTION 8

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity. Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity

Answer: C

NEW QUESTION 9

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database. What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database
- B. Update the application to read from the Multi-AZ standby instance
- C. Create a read replica and modify the application to use the appropriate endpoint
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C

NEW QUESTION 10

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID). What should a solutions architect do to meet these requirements?

- A. Launch the application on EC2 instances in each Availability Zone
- B. Attach EBS volumes to each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- E. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: C

NEW QUESTION 10

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput. Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone
- B. Launch the EC2 instances in a spread placement group in one Availability Zone
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

Answer: A

NEW QUESTION 13

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group
- B. Use a target tracking policy to dynamically scale the Auto Scaling group
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group

Answer: D

NEW QUESTION 17

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: B

NEW QUESTION 20

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Select TWO.)

- A. Ensure the root user uses a strong password
- B. Enable multi-factor authentication to the root user
- C. Store root user access keys in an encrypted Amazon S3 bucket
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document

Answer: AB

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

NEW QUESTION 24

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access. Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Answer: C

NEW QUESTION 29

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket.
- B. Use S3 event notifications to invoke microservice 2.
- C. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- D. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose.
- E. Implement code in microservice 2 to read from Kinesis Data Firehose.
- F. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Answer: C

NEW QUESTION 33

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

NEW QUESTION 36

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store

D. Amazon EBS Provisioned IOPS SSD (io1)

Answer: B

NEW QUESTION 37

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 41

A company has a three-tier image-sharing application it uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application

Which solution meets these requirements'?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layersMove the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer Move the database to a memory optimized instance type to store and serve users' images
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers Move the database to an Amazon RDS instance with a Multi-AZ deployment Use Amazon S3 to store and serve users' images

Answer: D

NEW QUESTION 43

Organizers for a global event want to put daily reports online as static HTML pages The pages are expected to generate millions of views from users around the world The files are stored in an Amazon S3 bucket A solutions architect has been asked to design an efficient and effective solution

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files
- B. Use cross-Region replication to all Regions
- C. Use the geoproximity feature of Amazon Route 53
- D. Use Amazon CloudFront with the S3 bucket as its origin

Answer: D

NEW QUESTION 47

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume For better scalability and availability the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone: placing both behind an Application Load Balancer After completing this change users reported that each time they refreshed the website they could see one subset of their documents or the other but never all of the documents at the same time What should a solutions architect propose to ensure users see all of their documents at once"

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers Return each document from the correct server

Answer: C

NEW QUESTION 52

A company runs an application on a group of Amazon Linux EC2 instances The application writes log files using standard API calls For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently

Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 53

A product team is creating a new application that will store a large amount of data The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances The application team believes the amount of space needed will continue to grow for the next 6 months

Which set of actions should a solutions architect take to support these needs'?

- A. Store the data in an Amazon EBS volume Mount the EBS volume on the application instances

- B. Store the data in an Amazon EFS file system Mount the file system on the application instances
- C. Store the data in Amazon S3 Glacier Update the vault policy to allow access to the application instances
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) Update the bucket policy to allow access to the application instances

Answer: B

NEW QUESTION 55

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

NEW QUESTION 60

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.
- B. Add Aurora Replicas
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 63

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on-premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD

NEW QUESTION 65

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

NEW QUESTION 66

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 69

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SAA-C02 Practice Exam Features:

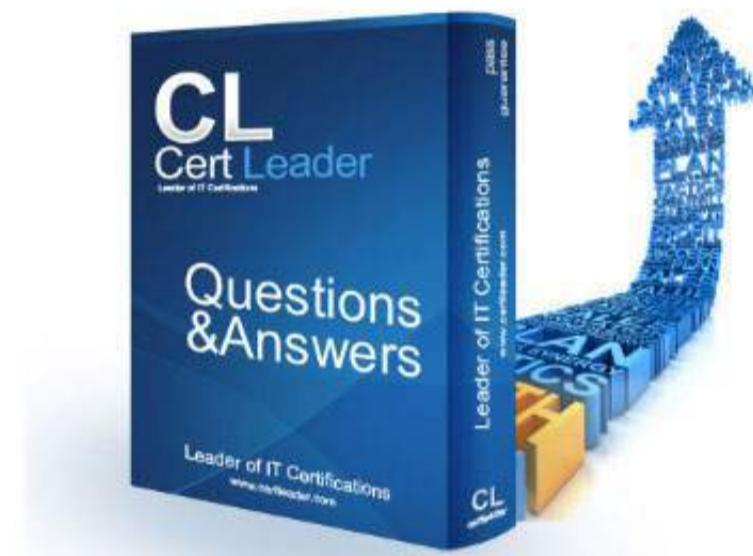
- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SAA-C02 Practice Test Here](#)

SAA-C02 Dumps

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.certleader.com/SAA-C02-dumps.html>



NEW QUESTION 1

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

NEW QUESTION 2

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Select TWO)

- A. Configure a VPC peering connection between the two VPC
- B. Access the API using the private address
- C. Configure an AWS Direct Connect connection between the two VPC
- D. Access the API using the private address.
- E. Configure a ClassicLink connection for the API into the client VPC Access the API using the ClassicLink address.
- F. Configure a PrivateLink connection for the API into the client VP
- G. Access the API using the PrivateLink address.
- H. Configure an AWS Resource Access Manager connection between the two accounts Access the API using the private address

Answer: DE

NEW QUESTION 3

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

Answer: C

NEW QUESTION 4

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company. How should security groups be configured in this situation? (Select TWO)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

Answer: AC

NEW QUESTION 5

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53, where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Answer: B

NEW QUESTION 6

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

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

Answer: A

NEW QUESTION 7

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

Answer: C

NEW QUESTION 8

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: B

NEW QUESTION 9

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy.
- E. Create alias records in Route 53 that point to the Application Load Balancer.

Answer: B

NEW QUESTION 10

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B

NEW QUESTION 10

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and

remove nodes based on the number of items in the SQS queue
D. Create an Amazon SNS topic to send the jobs that need to be processed Create an Amazon Machine Image (AMI) that consists of the processor application Create a launch template that uses the AMI Create an Auto Scaling group using the launch template Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C

NEW QUESTION 15

A company's application is running on Amazon EC2 instances in a single Region in the event of a disaster a solutions architect needs to ensure that the resources can also be deployed to a second Region
Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3
- B. Launch a new EC2 instance from an Amazon Machine image (AMI) in a new Region
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume

Answer: BD

NEW QUESTION 16

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: AD

NEW QUESTION 17

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: C

NEW QUESTION 20

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

Answer: C

NEW QUESTION 25

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances The database stores all data on multiple instances so it can withstand the loss of an instance The database requires block storage with latency and throughput to support several million transactions per second per server

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Answer: B

NEW QUESTION 30

A company currently operates a web application backed by an Amazon RDS MySQL database It has automated backups that are run daily and are not encrypted A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed The company will make at least one encrypted backup before destroying the old backups

What should be done to enable encryption for future backups?"

- A. Enable default encryption for the Amazon S3 bucket where backups are stored
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box
- C. Create a snapshot of the database Copy it to an encrypted snapshot Restore the database from the encrypted snapshot
- D. Enable an encrypted read replica on RDS for MySQL Promote the encrypted read replica to primary Remove the original database instance

Answer: C

NEW QUESTION 32

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months. Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume Mount the EBS volume on the application instances
- B. Store the data in an Amazon EFS file system Mount the file system on the application instances
- C. Store the data in Amazon S3 Glacier Update the vault policy to allow access to the application instances
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) Update the bucket policy to allow access to the application instances

Answer: B

NEW QUESTION 33

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.
- B. Add Aurora Replicas
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 35

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?"

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

Answer: D

NEW QUESTION 36

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3
- B. Use Amazon API Gateway with AWS Lambda
- C. Use Amazon QuickSight with Amazon Redshift
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics

Answer: D

NEW QUESTION 40

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies. How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Answer: D

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 45

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet. What should the solutions architect do to accomplish this? (Select TWO)

- A. Create a route table entry for the endpoint
- B. Create a gateway endpoint for DynamoDB
- C. Create a new DynamoDB table that uses the endpoint
- D. Create an ENI for the endpoint in each of the subnets of the VPC
- E. Create a security group entry in the default security group to provide access

Answer: AB

NEW QUESTION 47

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

100% Pass Your SAA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SAA-C02-dumps.html>

Exam Questions SAA-C02

AWS Certified Solutions Architect - Associate (SAA-C02)

<https://www.2passeeasy.com/dumps/SAA-C02/>



NEW QUESTION 1

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection. What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly.
- D. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- E. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.

Answer: D

NEW QUESTION 2

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

NEW QUESTION 3

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Answer: C

NEW QUESTION 4

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data must be stored in multiple AWS Regions.

How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

NEW QUESTION 5

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

NEW QUESTION 6

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only. What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

NEW QUESTION 7

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Answer: C

NEW QUESTION 8

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Answer: BD

NEW QUESTION 9

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Answer: C

NEW QUESTION 10

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage.

The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Select TWO)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Answer: BD

NEW QUESTION 10

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other but never all of the documents at the same time. What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Answer: C

NEW QUESTION 13

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently. Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

NEW QUESTION 14

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months. Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Answer: B

NEW QUESTION 17

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance. Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Answer: B

NEW QUESTION 22

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO)

- A. Add AWS Shield.
- B. Add Aurora Replicas
- C. Add AWS Direct Connect
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

Answer: DE

NEW QUESTION 26

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

NEW QUESTION 27

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on-premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD

NEW QUESTION 30

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAA-C02 Product From:

<https://www.2passeeasy.com/dumps/SAA-C02/>

Money Back Guarantee

SAA-C02 Practice Exam Features:

- * SAA-C02 Questions and Answers Updated Frequently
- * SAA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SAA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

Premium Dumps

Amazon AWS Certified Solutions Architect - Associate SAA-C02-Exam

SAA-C02 EXPERT VERIFIED CORRECTED 457 QUESTIONS & ANSWERS

Question #1

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's

DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Correct Answer: B

Active-passive failover -

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to

DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route

53 responds to DNS queries using the secondary record.

How Amazon Route 53 averts cascading failures

As a first defense against cascading failures, each request routing algorithm (such as weighted and failover) has a mode of last resort. In this special mode, when all records are considered unhealthy, the Route 53 algorithm reverts to considering all records healthy.

For example, if all instances of an application, on several hosts, are rejecting health check requests, Route 53 DNS servers will choose an answer anyway and return it rather than returning no DNS answer or returning an NXDOMAIN (non-existent domain) response. An application can respond to users but still fail health checks, so this provides some protection against misconfiguration.

Similarly, if an application is overloaded, and one out of three endpoints fails its health checks, so that it's excluded from Route 53 DNS responses, Route 53 distributes responses between the two remaining endpoints. If the remaining endpoints are unable to handle the additional load and they fail, Route 53 reverts to distributing requests to all three endpoints.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html> <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-problems.html>

Question #2

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Correct Answer: A

Placement groups -

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Depending on the type of workload.

Cluster " packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Question #3

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world.

Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: C A

Reference:

<https://aws.amazon.com/ec2/autoscaling/>

Question #4

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm. Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Correct Answer: B

Migrating Existing Files to Amazon FSx for Windows File Server Using AWS DataSync

We recommend using AWS DataSync to transfer data between Amazon FSx for Windows File Server file systems. DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and other AWS storage services over the internet or

AWS Direct Connect. DataSync can transfer your file system data and metadata, such as ownership, time stamps, and access permissions.

Reference:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

Question #5

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Correct Answer: D

Question #6

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda

- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Correct Answer: BD DE

Kinesis Data Streams and Kinesis Client Library (KCL) – Data from the data source can be continuously captured and streamed in near real-time using Kinesis

Data Streams. With the Kinesis Client Library (KCL), you can build your own application that can preprocess the streaming data as they arrive and emit the data for generating incremental views and downstream analysis. Kinesis Data Analytics – This service provides the easiest way to process the data that is streaming through Kinesis Data Stream or Kinesis Data Firehose using SQL. This enables customers to gain actionable insight in near real-time from the incremental stream before storing it in Amazon S3.

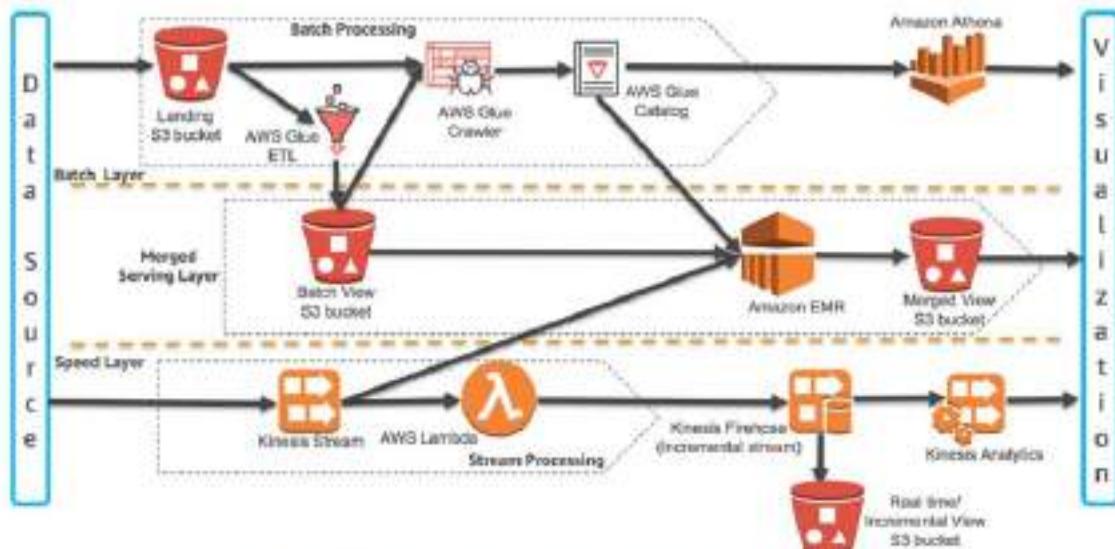


Figure 2: Lambda Architecture Building Blocks on AWS

Reference:

<https://d1.awsstatic.com/whitepapers/lambda-architecure-on-for-batch-aws.pdf>

Question #7

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C

Scheduled Scaling for Amazon EC2 Auto Scaling

Scheduled scaling allows you to set your own scaling schedule. For example, let's say that every week the traffic to your web application starts to increase on

Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Question #8

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Choose two.)

- A. Add AWS Shield.
- B. Add Aurora Replica.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Correct Answer: DE

AWS Global Accelerator - **BE**

Acceleration for latency-sensitive applications

Many applications, especially in areas such as gaming, media, mobile apps, and financials, require very low latency for a great user experience. To improve the user experience, Global Accelerator directs user traffic to the application endpoint that is nearest to the client, which reduces internet latency and jitter. Global

Accelerator routes traffic to the closest edge location by using Anycast, and then routes it to the closest regional endpoint over the AWS global network. Global

Accelerator quickly reacts to changes in network performance to improve your users' application performance.

Amazon CloudFront -

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

Question #9

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Correct Answer: C

Amazon RDS Read Replicas -

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as

Amazon Aurora.

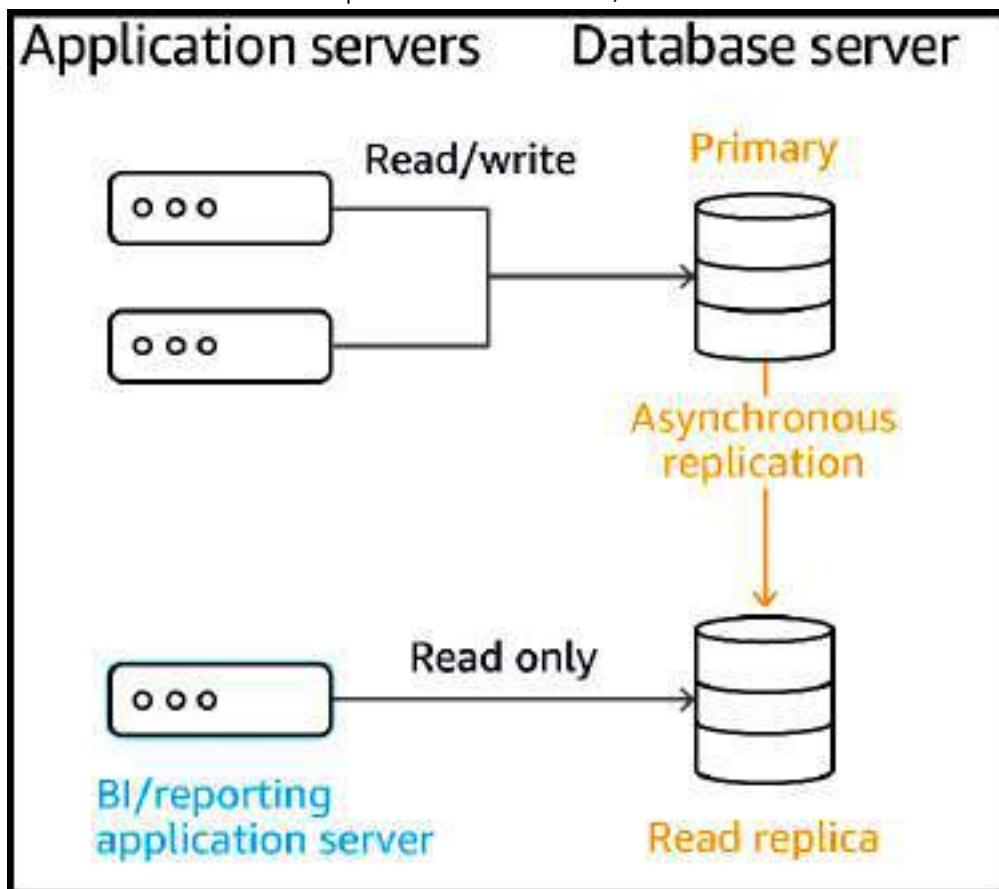
For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source

DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance.

Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon

Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the online documentation.



Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html <https://aws.amazon.com/rds/features/read-replicas/>

Question #10

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity.
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Correct Answer: C

Reference:

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html <https://aws.amazon.com/directconnect/>

Question #11

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Correct Answer: C

"block access for certain countries." You can use geo restriction, also known as geo blocking, to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

Question #12

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.
- D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Correct Answer: B

Amazon Elastic File System -

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as

you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include: big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

Reference:

<https://aws.amazon.com/efs/>

Question #13

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Correct Answer: C

Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Starting today, Amazon RDS Read Replicas for MySQL and MariaDB now support Multi-AZ deployments. Combining Read Replicas with Multi-AZ enables you to build a resilient disaster recovery strategy and simplify your database engine upgrade process.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

You can also combine Read Replicas with Multi-AZ for your database engine upgrade process. You can create a Read Replica of your production database instance and upgrade it to a new database engine version. When the upgrade is complete, you can stop applications, promote the Read Replica to a standalone database instance, and switch over your applications. Since the database instance is already a Multi-AZ deployment, no additional steps are needed.

Overview of Amazon RDS Read Replicas

Deploying one or more read replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more read replicas.

Serving read traffic while the source DB instance is unavailable. In some cases, your source DB instance might not be able to take I/O requests, for example due to I/O suspension for backups or scheduled maintenance. In these cases, you can direct read traffic to your read replicas. For this use case, keep in mind that the data on the read replica might be "stale" because the source DB instance is unavailable.

Business reporting or data warehousing scenarios where you might want business reporting queries to run against a read replica, rather than your primary, production DB instance.

Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the source DB instance fails.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #14

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Correct Answer: B

Question #15

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Correct Answer: D

Using Amazon S3 Origins, MediaPackage Channels, and Custom Origins for Web Distributions

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

Using Amazon S3 Buckets Configured as Website Endpoints for Your Origin

You can set up an Amazon S3 bucket that is configured as a website endpoint as custom origin with CloudFront.

When you configure your CloudFront distribution, for the origin, enter the Amazon S3 static website hosting endpoint for your bucket. This value appears in the

Amazon S3 console, on the Properties tab, in the Static website hosting pane. For example: <http://bucket-name.s3-website-region.amazonaws.com>

For more information about specifying Amazon S3 static website endpoints, see Website endpoints in the Amazon Simple Storage Service Developer Guide.

When you specify the bucket name in this format as your origin, you can use Amazon S3 redirects and Amazon S3 custom error documents. For more information about Amazon S3 features, see the Amazon S3 documentation.

Using an Amazon S3 bucket as your CloudFront origin server doesn't change it in any way. You can still use it as you normally would and you incur regular

Amazon S3 charges.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #16

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Correct Answer: BC

Reference:

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-api-gateway-supports-endpoint-integrations-with-private-vpcs>

Question #17

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.

D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Correct Answer: C

Register endpoints for endpoint groups: You register one or more regional resources, such as Application Load Balancers, Network Load Balancers, EC2

Instances, or Elastic IP addresses, in each endpoint group. Then you can set weights to choose how much traffic is routed to each endpoint. Endpoints in AWS Global Accelerator

Endpoints in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. A static IP address serves as a single point of contact for clients, and Global Accelerator then distributes incoming traffic across healthy endpoints. Global Accelerator directs traffic to endpoints by using the port (or port range) that you specify for the listener that the endpoint group for the endpoint belongs to.

Each endpoint group can have multiple endpoints. You can add each endpoint to multiple endpoint groups, but the endpoint groups must be associated with different listeners.

Global Accelerator continually monitors the health of all endpoints that are included in an endpoint group. It routes traffic only to the active endpoints that are healthy. If Global Accelerator doesn't have any healthy endpoints to route traffic to, it routes traffic to all endpoints.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints.html> <https://aws.amazon.com/global-accelerator/faqs/>

Question #18

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Correct Answer: B

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume — there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service — all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging. All you need to do is supply your code in one of the languages that AWS Lambda supports.

Storing your static content with S3 provides a lot of advantages. But to help optimize your application's performance and security while effectively managing cost, we recommend that you also set up Amazon CloudFront to work with your S3 bucket to serve and protect the content. CloudFront is a content delivery network

(CDN) service that delivers static and dynamic web content, video streams, and APIs around the world, securely and at scale. By design,

delivering data out of

CloudFront can be more cost effective than delivering it from S3 directly to your users.

CloudFront serves content through a worldwide network of data centers called Edge Locations. Using edge servers to cache and serve content improves performance by providing content closer to where viewers are located. CloudFront has edge servers in locations all around the world.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

Question #19

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Correct Answer: C

Reference:

<https://medium.com/@KerrySheldon/s3-exercise-2-4-adding-objects-to-an-s3-bucket-with-cross-region-replication-a78b332b7697>

Question #20

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

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

Correct Answer: B

Question #21

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.

- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Correct Answer: A

Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of

DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections. Applications connect to a read replica the same way they do to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #22

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD

Question #23

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Correct Answer: BD

Cross Region EC2 AMI Copy -

We know that you want to build applications that span AWS Regions and we're working to provide you with the services and features needed to do so. We started out by launching the EBS Snapshot Copy feature late last year. This feature gave you the ability to copy a snapshot from Region to Region with just a couple of clicks. In addition, last month we made a significant reduction (26% to 83%) in the cost of transferring data between AWS Regions, making it less expensive to operate in more than one AWS region.

Today we are introducing a new feature: Amazon Machine Image (AMI) Copy. AMI Copy enables you to easily copy your Amazon Machine Images between AWS

Regions. AMI Copy helps enable several key scenarios including:

Simple and Consistent Multi-Region Deployment – You can copy an AMI from one region to another, enabling you to easily launch consistent instances based on the same AMI into different regions.

Scalability – You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location.

Performance – You can increase performance by distributing your application and locating critical components of your application in closer proximity to your users.

You can also take advantage of region-specific features such as instance types or other AWS services.

Even Higher Availability – You can design and deploy applications across AWS regions, to increase availability.

Once the new AMI is in an Available state the copy is complete.

Reference:

<https://aws.amazon.com/blogs/aws/ec2-ami-copy-between-regions/>

Question #24

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.

What should the solutions architect do to accomplish this? (Choose two.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Correct Answer: AB

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Gateway endpoints -

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3 -

DynamoDB -

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Question #25

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the over to the new master. Delete the old RDS instance.

Correct Answer: C

How do I encrypt Amazon RDS snapshots?

The following steps are applicable to Amazon RDS for MySQL, Oracle, SQL Server, PostgreSQL, or MariaDB.

Important: If you use Amazon Aurora, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster if you specify an AWS Key.

Management Service (AWS KMS) encryption key when you restore from the unencrypted DB cluster snapshot. For more information, see Limitations of Amazon

RDS Encrypted DB Instances.

Open the Amazon RDS console, and then choose Snapshots from the navigation pane.

Select the snapshot that you want to encrypt.

Under Snapshot Actions, choose Copy Snapshot.

Choose your Destination Region, and then enter your New DB Snapshot Identifier.

Change Enable Encryption to Yes.

Select your Master Key from the list, and then choose Copy Snapshot.

After the snapshot status is available, the Encrypted field will be True to indicate that the snapshot is encrypted.

You now have an encrypted snapshot of your DB. You can use this encrypted DB snapshot to restore the DB instance from the DB snapshot.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-rds-snapshots/>

Question #26

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Correct Answer: D A

Question #27

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.

Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Correct Answer: A

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Routing traffic to an Amazon CloudFront web distribution by using your domain name.

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website—including dynamic, static, streaming, and interactive content—by using a global network of edge locations. Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

To use CloudFront to distribute your content, you create a web distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want

CloudFront to get your content from, whether you want only selected users to have access to your content, and whether you want to require users to use HTTPS.

When you create a web distribution, CloudFront assigns a domain name to the distribution, such as `asd11111abcdef8.cloudfront.net`. You can use this domain name in the URLs for your content, for example:

[1]

Alternatively, you might prefer to use your own domain name in URLs, for example:

[1]

If you want to use your own domain name, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. An alias record is a Route

53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as `example.com`, and for subdomains, such as `www.example.com`. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html> <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #28

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions.
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Correct Answer: C

AWS Lambda -

With Lambda, you can run code for virtually any type of application or backend service – all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

How it works -



Amazon API Gateway -

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and

WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

Reference:

<https://aws.amazon.com/lambda/>

<https://aws.amazon.com/api-gateway/>

Question #29

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of

the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances

Correct Answer: D

Explanation -

C

Scheduled Reserved Instances -

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled

Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

If you require a capacity reservation on a continuous basis, Reserved Instances might meet your needs and decrease costs.

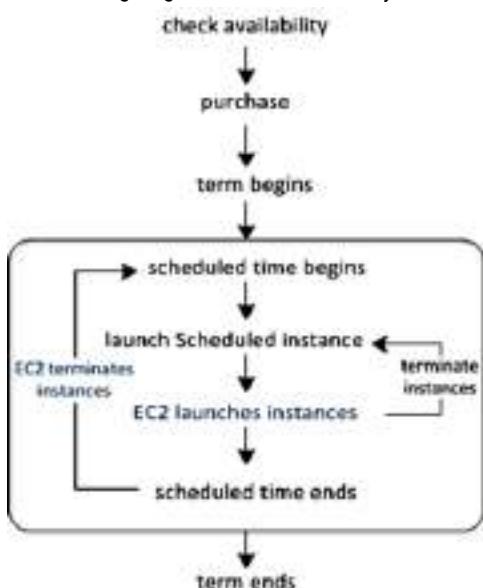
How Scheduled Instances Work -

Amazon EC2 sets aside pools of EC2 instances in each Availability Zone for use as Scheduled Instances. Each pool supports a specific combination of instance type, operating system, and network.

To get started, you must search for an available schedule. You can search across multiple pools or a single pool. After you locate a suitable schedule, purchase it.

You must launch your Scheduled Instances during their scheduled time periods, using a launch configuration that matches the following attributes of the schedule that you purchased: instance type, Availability Zone, network, and platform. When you do so, Amazon EC2 launches EC2 instances on your behalf, based on the specified launch specification. Amazon EC2 must ensure that the EC2 instances have terminated by the end of the current scheduled time period so that the capacity is available for any other Scheduled Instances it is reserved for. Therefore, Amazon EC2 terminates the EC2 instances three minutes before the end of the current scheduled time period.

You can't stop or reboot Scheduled Instances, but you can terminate them manually as needed. If you terminate a Scheduled Instance before its current scheduled time period ends, you can launch it again after a few minutes. Otherwise, you must wait until the next scheduled time period. The following diagram illustrates the lifecycle of a Scheduled Instance.



Reference:

Question #30

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.

What should a solutions architect do to meet these requirements? (Choose two.)?

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Correct Answer: CE

Network Load Balancer overview -

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.

When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. For more information, see Availability Zones.

If you enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone, this increases the fault tolerance of your applications. For example, if one or more target groups does not have a healthy target in an Availability Zone, we remove the

IP address for the corresponding subnet from DNS, but the load balancer nodes in the other Availability Zones are still available to route traffic. If a client doesn't honor the time-to-live (TTL) and sends requests to the IP address after it is removed from DNS, the requests fail.

For TCP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, destination port, and TCP sequence number. The TCP connections from a client have different source ports and sequence numbers, and can be routed to different targets. Each individual TCP connection is routed to a single target for the life of the connection.

For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html> <https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

Question #31

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Correct Answer: C

However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

DB instances that are encrypted can't be modified to disable encryption.

You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.

Encrypted read replicas must be encrypted with the same key as the source DB instance when both are in the same AWS Region.

You can't restore an unencrypted backup or snapshot to an encrypted DB instance.

To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key identifier of the destination AWS Region. This is because KMS encryption keys are specific to the AWS Region that they are created in.

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Question #32

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Correct Answer: C

Reference:

[\(geolocation routing\)](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Question #33

A solutions architect has created a new AWS account and must secure AWS account root user access.

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

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: AB

Question #34

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B

S3 Intelligent-Tiering -

S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers – frequent access and infrequent access – when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the

S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.99999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/>

Question #35

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website. What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Correct Answer: B

If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those IP addresses.

AWS Web Application Firewall (WAF) " Helps to protect your web applications from common application-layer exploits that can affect availability or consume excessive resources. As you can see in my post (New " AWS WAF), WAF allows you to use access control lists (ACLs), rules, and conditions that define acceptable or unacceptable requests or IP addresses. You can selectively allow or deny access to specific parts of your web application and you can also guard against various SQL injection attacks. We launched WAF with support for Amazon CloudFront.

Reference:

<https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-loadbalancers/> <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-ip-conditions.html> <https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-load-balancers/>

Question #36

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Correct Answer: C

A

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

Question #37

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.

D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Correct Answer: C

Working with cross-site scripting match conditions

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF Classic to inspect for possible malicious scripts. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious scripts.

Web Application Firewall -

You can now use AWS WAF to protect your web applications on your Application Load Balancers. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html> <https://aws.amazon.com/elasticloadbalancing/features/>

Question #38

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage. There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly when the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Correct Answer: D

Amazon RDS Read Replicas -

Enhanced performance -

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Because read replicas can be promoted to master status, they are useful as part of a sharding implementation.

To further maximize read performance, Amazon RDS for MySQL allows you to add table indexes directly to Read Replicas, without those indexes being present on the master.

Reference:

<https://aws.amazon.com/rds/features/read-replicas>

Question #39

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application

Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 AutoScaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to: Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your AutoScaling group.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Question #40

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to

2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: A

C

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

Question #41

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.

Which changes should be made to the database tier to improve performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.

C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.

D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Correct Answer: D

Question #42

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution.

What should a solutions architect do to accomplish this?

A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.

B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.

C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.

D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Correct Answer: B

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket.

You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html> <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #43

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon EBS Provisioned IOPS SSD (io1)

Correct Answer: B

Explanation -

Amazon FSx for Lustre -

Amazon FSx for Lustre is a new, fully managed service provided by AWS based on the Lustre file system. Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

FSx for Lustre allows customers to create a Lustre filesystem on demand and associate it to an Amazon S3 bucket. As part of the filesystem creation, Lustre reads the objects in the buckets and adds that to the file system metadata. Any Lustre client in your VPC is then able to access the data, which gets cached on the high-speed Lustre filesystem. This is ideal for HPC workloads, because you can get the speed of an optimized Lustre file system without having to manage the complexity of deploying, optimizing, and managing the Lustre cluster.

Additionally, having the filesystem work natively with Amazon S3 means you can shut down the Lustre filesystem when you don't need it but still access objects in

Amazon S3 via other AWS Services. FSx for Lustre also allows you to also write the output of your HPC job back to Amazon S3.

Reference:

https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf

(p.8)

Question #44

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.

What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
- B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.
- C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Correct Answer: A

AWS Managed Microsoft AD -

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2012 R2. When you select and launch this directory type, it is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC). The domain controllers run in different Availability Zones in a region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you.

Reference:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

Question #45

A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

- A. Enable Amazon S3 versioning.
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy.
- D. Enable Amazon S3 cross-Region replication.

Correct Answer: A

Data can be recover if versioning enable, also it provide a extra protection like file delete,MFA delete. MFA. Delete only works for CLI or API interaction, not in the

AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Reference:

<https://books.google.com.sg/books?id=wv45DQAAQBAJ&pg=PA39&lpg=PA39&dq=hosts+a+static+website+within+an+Amazon+S3+bucket.+A+solutions+architect+needs+to+ensure+that+data+can+be+recovered+in+case+of+accidental+deletion&source=bl&ots=0NolP5igY5&sig=ACfU3U3opL9Jha6jM2El8x7EcjK4rigQHQ&hl=en&sa=X&ved=2ahUKEwiS9e3yy7vpAhVx73MBHZNoDnQQ6AEwAH oECBQQAQ#v=onepage&q=hosts%20a%20static%20website%20within%20an%20Amazon%20S3%20bucket.%20A%20solutions%20architect%20needs%20to%20ensure%20that%20data%20can%20be%20recovered%20in%20case%20of%20accidental%20deletion&f=false https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/ https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html>

Question #46

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Correct Answer: B

Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/#:~>

Question #47

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Correct Answer: B

AWS Storage Gateway Hardware Appliance

Hardware Appliance -

Storage Gateway is available as a hardware appliance, adding to the existing support for VMware ESXi, Microsoft Hyper-V, and Amazon EC2.

This means that you can now make use of Storage Gateway in situations where you do not have a virtualized environment, server-class hardware or IT staff with the specialized skills that are needed to manage them. You can order appliances from Amazon.com for delivery to branch offices, warehouses, and ~~outpost~~ offices that lack dedicated IT resources. Setup (as you will see in a minute) is quick and easy, and gives you access to three storage solutions:

File Gateway – A file interface to Amazon S3, accessible via NFS or SMB. The files are stored as S3 objects, allowing you to make use of specialized S3 features such as lifecycle management and cross-region replication. You can trigger AWS Lambda functions, run Amazon Athena queries, and use Amazon Macie to discover and classify sensitive data.

Reference:

<https://aws.amazon.com/blogs/aws/new-aws-storage-gateway-hardware-appliance/> <https://aws.amazon.com/storagegateway/file/>

Question #48

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

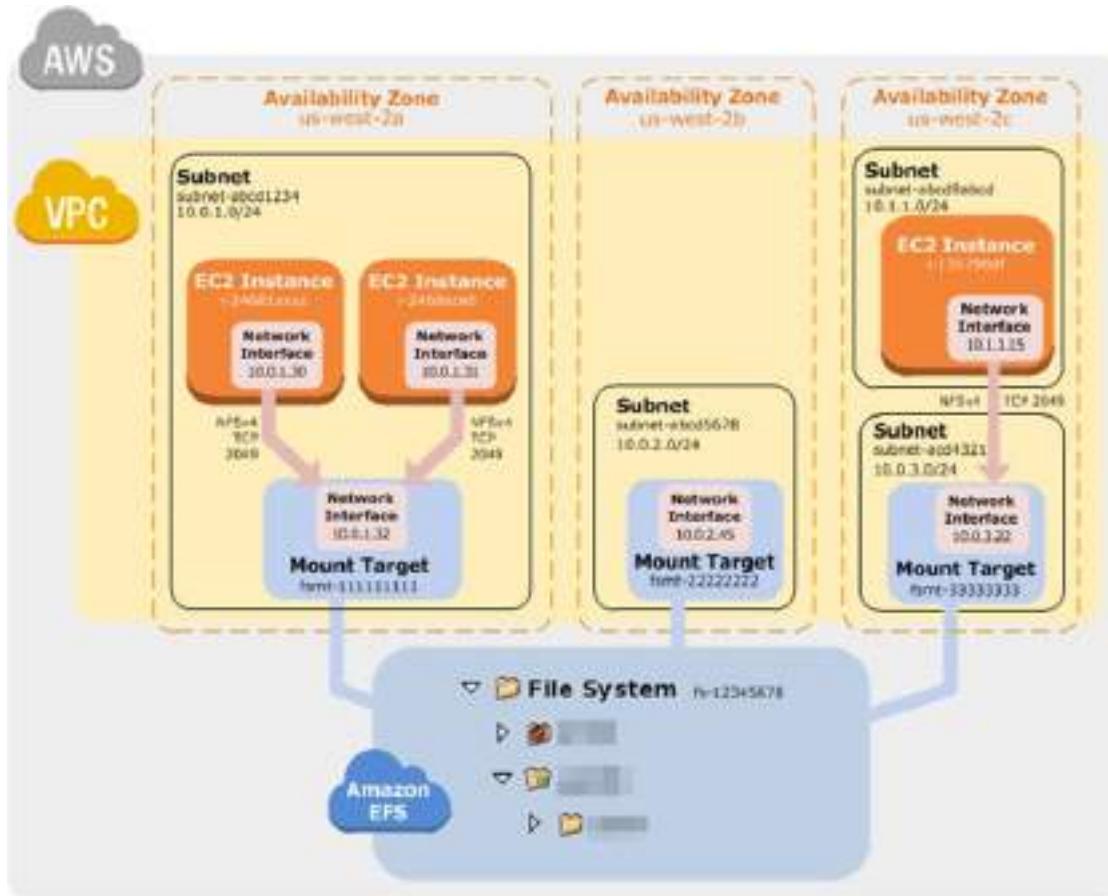
- A. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
- B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C

How Amazon EFS Works with Amazon EC2

The following illustration shows an example VPC accessing an Amazon EFS file system. Here, EC2 instances in the VPC have file systems mounted.

In this illustration, the VPC has three Availability Zones, and each has one mount target created in it. We recommend that you access the file system from a mount target within the same Availability Zone. One of the Availability Zones has two subnets. However, a mount target is created in only one of the subnets.



Benefits of Auto Scaling -

Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Amazon EC2 Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Amazon EC2 Auto Scaling can launch instances in another one to compensate.

Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of capacity to handle the current traffic demand.

Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you save money by launching instances when they are needed and terminating them when they aren't.

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2> <https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

Question #49

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations.

The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Correct Answer: D

Service Control Policy concepts -

SCPs offer central access controls for all IAM entities in your accounts. You can use them to enforce the permissions you want everyone in your business to follow. Using SCPs, you can give your developers more freedom to manage their own permissions because you know they can only operate within the boundaries you define.

You create and apply SCPs through AWS Organizations. When you create an organization, AWS Organizations automatically creates a root, which forms the parent container for all the accounts in your organization. Inside the root, you can group accounts in your organization into organizational units (OUs) to simplify management of these accounts. You can create multiple OUs within a single organization, and you can create OUs within other OUs to form a hierarchical structure. You can attach SCPs to the organization root, OUs, and individual accounts. SCPs attached to the root and OUs apply to all OUs and accounts inside of them.

SCPs use the AWS Identity and Access Management (IAM) policy language; however, they do not grant permissions. SCPs enable you set permission guardrails by defining the maximum available permissions for IAM entities in an account. If a SCP denies an action for an account, none of the entities in the account can take that action, even if their IAM permissions allow them to do so. The guardrails set in SCPs apply to all

IAM entities in the account, which include all users, roles, and the account root user.

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-aws-organization/>

#:<~:text=Central%20security%20administrators%20use%20service,users%20and%20roles)%20adhere%20to.&text=Now%2C%20using%20SCPs%2C%20you%

20can,your%20organization%20or%20organizational%20unit

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Question #50

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.

What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering

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

Correct Answer: B

Reference:

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

Question #51

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Correct Answer: C

Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and

4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu

AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools.

For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For some AMIs, you'll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see Installing the NFS Client.

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

How Amazon EFS Works with Amazon EC2



Question #52

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Correct Answer: D

"Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom."

Server-Side Encryption: Using SSE-KMS

You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSE-S3, SSE-C, or SSE-KMS.

SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see Protecting Data Using Server-Side

Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

SSE-C requires that you manage the encryption key. For more information about SSE-C, see Protecting Data Using Server-Side Encryption with Customer-

Provided Encryption Keys (SSE-C).

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS.

The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

You can request encryption and select a CMK by using the Amazon S3 console or API. In the console, check the appropriate box to perform encryption and select your CMK from the list. For the Amazon S3 API, specify encryption and choose your CMK by setting the appropriate headers in a GET or PUT request.

Reference:

<https://aws.amazon.com/kms/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html> <https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

Question #53

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Correct Answer: D

Reserved Instances -

Having 50 EC2 RIs provide a discounted hourly rate and an optional capacity reservation for EC2 instances. AWS Billing automatically applies your RI's discounted rate when attributes of EC2 instance usage match attributes of an active RI.

If an Availability Zone is specified, EC2 reserves capacity matching the attributes of the RI. The capacity reservation of an RI is automatically utilized by running instances matching these attributes.

You can also choose to forego the capacity reservation and purchase an RI that is scoped to a region. RIs that are scoped to a region automatically apply the RI's discount to instance usage across AZs and instance sizes in a region, making it easier for you to take advantage of the RI's discounted rate.

On-Demand Instance -

On-Demand instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

The pricing below includes the cost to run private and public AMIs on the specified operating system (Windows Usage prices apply to Windows Server 2003 R2,

2008, 2008 R2, 2012, 2012 R2, 2016, and 2019). Amazon also provides you with additional instances for Amazon EC2 running Microsoft Windows with SQL

Server, Amazon EC2 running SUSE Linux Enterprise Server, Amazon EC2 running Red Hat Enterprise Linux and Amazon EC2 running IBM that are priced differently.

Spot Instances -

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your

Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

<https://aws.amazon.com/ec2/pricing/on-demand/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

Question #54

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

- A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.

- B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
- C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.
- E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Correct Answer: DE AE

Question #55

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection.

What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket policy to enforce a VPC endpoint.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Correct Answer: B D

Question #56

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Choose two.)

- A. Create new public and private subnets in the same AZ for high availability.
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.
- E. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Correct Answer: BE

Question #57

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

To customize your data retention approach and control storage costs, use object versioning with Object lifecycle management. For information about creating S3

Lifecycle policies using the AWS Management Console, see How Do I Create a Lifecycle Policy for an S3 Bucket? in the Amazon Simple Storage Service Console

User Guide.

If you have an object expiration lifecycle policy in your non-versioned bucket and you want to maintain the same permanent delete behavior when you enable versioning, you must add a noncurrent expiration policy. The noncurrent expiration lifecycle policy will manage the deletes of the noncurrent object versions in the version-enabled bucket. (A version-enabled bucket maintains one current and zero or more noncurrent object versions.)

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key. Enabling and suspending versioning is done at the bucket level. When you enable versioning on an existing bucket, objects that are already stored in the bucket are unchanged. The version IDs (null), contents, and permissions remain the same. After you enable S3 Versioning for a bucket, each object that is added to the bucket gets a version ID, which distinguishes it from other versions of the same key.

Only Amazon S3 generates version IDs, and they can't be edited. Version IDs are Unicode, UTF-8 encoded, URL-ready, opaque strings that are no more than

1,024 bytes long. The following is an example: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dlbrHY+MTRCx3vjVBH40Nr8X8gdRQBpUMLUo.

Using MFA delete -

If a bucket's versioning configuration is MFA Delete-enabled, the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket. Requests that include x-amz-mfa must use HTTPS. The header's value is the concatenation of your authentication device's serial number, a space, and the authentication code displayed on it. If you do not include this request header, the request fails.

Reference:

<https://aws.amazon.com/s3/features/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html> <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Question #58

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.

What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Correct Answer: C

Share an object with others -

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method

(GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.

Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

Question #59

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: AC

Question #60

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM activity across all account in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Correct Answer: D

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Question #61

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an

Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application. Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: B

Expanding Your Scaled and Load-Balanced Application to an Additional Availability Zone.

When one Availability Zone becomes unhealthy or unavailable, Amazon EC2 Auto Scaling launches new instances in an unaffected zone. When the unhealthy

Availability Zone returns to a healthy state, Amazon EC2 Auto Scaling automatically redistributes the application instances evenly across all of the zones for your

Auto Scaling group. Amazon EC2 Auto Scaling does this by attempting to launch new instances in the Availability Zone with the fewest instances. If the attempt fails, however, Amazon EC2 Auto Scaling attempts to launch in other Availability Zones until it succeeds.

You can expand the availability of your scaled and load-balanced application by adding an Availability Zone to your Auto Scaling group and then enabling that zone for your load balancer. After you've enabled the new Availability Zone, the load balancer begins to route traffic equally among all the enabled zones.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

Question #62

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.

Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Correct Answer: D

Amazon S3 -

Requests to Amazon S3 can be authenticated or anonymous. Authenticated access requires credentials that AWS can use to authenticate your requests. When making REST API calls directly from your code, you create a signature using valid credentials and include the signature in your request. Amazon Simple Storage

Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means

customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Reference:

<https://aws.amazon.com/s3/>

Question #63

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL.
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Correct Answer: C

In-memory databases on AWS Amazon ElastiCache for Redis.

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides submillisecond latency to power internet-scale, real-time applications.

Developers can use ElastiCache for Redis as an in-memory nonrelational database. The ElastiCache for Redis cluster configuration supports up to 15 shards and enables customers to run Redis workloads with up to 6.1 TB of in-memory capacity in a single cluster. ElastiCache for Redis also provides the ability to add and remove shards from a running cluster. You can dynamically scaleout and even scale in your Redis cluster workloads to adapt to changes in demand.

Reference:

<https://aws.amazon.com/elasticache/redis/faqs/>

<https://aws.amazon.com/nosql/in-memory/>

Question #64

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an

Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.

What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Correct Answer: A

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined — such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

As an example, suppose that you're serving an image from a traditional web server, not from CloudFront. For example, you might serve an image,

[1]

Your users can easily navigate to this URL and see the image. But they probably don't know that their request was routed from one network to another — through the complex collection of interconnected networks that comprise the internet — until the image was found.

CloudFront speeds up the distribution of your content by routing each user request through the AWS backbone network to the edge location that can best serve your content. Typically, this is a CloudFront edge server that provides the fastest delivery to the viewer. Using the AWS network dramatically reduces the number of networks that your users' requests must pass through, which improves performance. Users get lower latency — the time it takes to load the first byte of the file — and higher data transfer rates.

You also get increased reliability and availability because copies of your files (also known as objects) are now held (or cached) in multiple edge locations around the world.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #65

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C

Amazon Simple Queue Service -

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices,

distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

Scaling Based on Amazon SQS -

There are some scenarios where you might think about scaling in response to activity in an Amazon SQS queue. For example, suppose that you have a web app that lets users upload images and use them online. In this scenario, each image requires resizing and encoding before it can be published. The app runs on EC2 instances in an Auto Scaling group, and it's configured to handle your typical upload rates. Unhealthy instances are terminated and replaced to maintain current instance levels at all times. The app places the raw bitmap data of the images in an SQS queue for processing. It processes the images and then publishes the processed images where they can be viewed by users. The architecture for this scenario works well if the number of image uploads doesn't vary over time. But if the number of uploads changes over time, you might consider using dynamic scaling to scale the capacity of your Auto Scaling group.

Reference:

<https://aws.amazon.com/sqs/#:~:text=Amazon%20SQS%20leverages%20the%20AWS,queues%20provide%20nearly%20unlimited%20throughput>
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Question #66

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
- D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

Correct Answer: C

Question #67

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow.

Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Correct Answer: A

Reference:

Question #68

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Correct Answer: B

Question #69

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon

RDS table, and deletes -

the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages. What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Correct Answer: D

Question #70

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

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

What is the effect of this policy?

Question #71

C

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

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

Correct Answer: A

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

Question #72

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the

MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the

database to a memory optimized instance type to store and serve user's images.

D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve user's images.

Correct Answer: D

Question #73

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Correct Answer: D B

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Question #74

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon

EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Correct Answer: D

Question #75

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance. Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Correct Answer: *B* **C**

Question #76

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Correct Answer: *D*

Reference:

<https://aws.amazon.com/kinesis/data-analytics/>

Question #77

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

Correct Answer: B

Question #78

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.
- D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Correct Answer: B

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

Question #79

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Correct Answer: A

Question #80

A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution's cost should be minimal.

Which storage solution meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: D

Question #81

A company's operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.

Which solution would satisfy these requirements?

- A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.
- B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.
- C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
- D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

Correct Answer: D

Question #82

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Correct Answer: A

Question #83

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences. The application is successful with a rapid increase in the number of users every month.

The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because

the single Amazon

RDS for MySQL instance has triggered alarms related to resource exhaustion due to read requests.

What can a solutions architect recommend to prevent service interruptions at the database layer with minimal changes to code?

- A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.
- B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

Correct Answer: A

Question #84

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

Question #85

A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.

Which solution should a solutions architect recommend that is MOST highly available?

- A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
- B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
- C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
- D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Correct Answer: C

Question #86

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.

What should a solutions architect recommend?

- A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.
- D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Correct Answer: A

Question #87

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Execute a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Correct Answer: B

Question #88

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.

- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Correct Answer: A

Question #89

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Correct Answer: B

Question #90

A public-facing web application queries a database hosted on an Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.

What should a solutions architect recommend to the application team? (Choose two.)

- A. Cache query data in Amazon SQS
- B. Create a read replica to offload queries
- C. Migrate the database to Amazon Athena
- D. Implement Amazon DynamoDB Accelerator to cache data.
- E. Migrate the database to Amazon RDS

Correct Answer: BE

Question #91

A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

- A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.

- B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
- C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
- D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Correct Answer: C

Question #92

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on

Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.

What should a solutions architect recommend?

- A. Configure an Amazon Route 53 latency routing policy.
- B. Configure an Amazon Route 53 geolocation routing policy.
- C. Configure an Amazon Route 53 geoproximity routing policy.
- D. Configure an Amazon Route 53 multivalue answer routing policy.

Correct Answer: C

Question #93

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share.

Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.

What should a solutions architect recommend to meet these requirements?

- A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.
- B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.
- C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
- D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Correct Answer: D

Question #94

An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.

Which solution is the MOST cost-effective?

- A. DEV with Spot Instances and PROD with On-Demand Instances

- B. DEV with On-Demand Instances and PROD with Spot Instances
- C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
- D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Correct Answer: C No correct answer

Question #95

A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage.

How can this be achieved?

- A. Create an Amazon EFS file system and mount it from each EC2 instance.
- B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.
- C. Create a file system on an Amazon EBS Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.
- D. Create file systems on Amazon EBS volumes attached to each EC2 instance. Synchronize the Amazon EBS volumes across the different EC2 instances.

Correct Answer: A

Question #96

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: C

Question #97

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an

S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.

Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide

access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.

- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Correct Answer: C

Question #98

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.

Which database implementations will meet these requirements? (Choose two.)

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon RDS for MySQL
- D. MySQL-compatible Amazon Aurora Multi-AZ
- E. Amazon RDS for SQL Server Standard Edition Multi-AZ

Correct Answer: DE

Question #99

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Correct Answer: C

Reference:

<https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/>

Question #100

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

```

Policy1
{
    "Version": "2012-10-17", "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam>List*",
                "kms>List*",
                "ec2:*",
                "ds:*",
                "logs:Get*",
                "logs:Describe*"
            ],
            "Resource": "*"
        }
    ]
}

Policy2
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ds>Delete*",
            "Resource": "*"
        }
    ]
}

```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

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

Correct Answer: C

Question #101

A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connections to it.

How can a solutions architect achieve this objective?

- A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
- B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
- C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
- D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

Correct Answer: B

Question #102

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

Correct Answer: A

Question #103

A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

- A. Use step scaling.
- B. Use simple scaling.
- C. Use lifecycle hooks.
- D. Use scheduled scaling.

Correct Answer: D

Question #104

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B

Question #105

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to

AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
- C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
- D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Correct Answer: B

Question #106

A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis.

What is the MOST cost-effective storage solution alternative to the current configuration?

- A. Configure a lifecycle policy to delete the objects after 30 days.
- B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
- C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Correct Answer: D

Question #107

A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited time.

What should a solutions architect do to securely meet these requirements?

- A. Enable public access on an Amazon S3 bucket.
- B. Generate a presigned URL to share with the users.
- C. Encrypt files using AWS KMS and provide keys to the users.
- D. Create and assign IAM roles that will grant GetObject permissions to the users.

Correct Answer: B

Question #108

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an

NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing.

Which solution will meet these requirements?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
- B. Use an AWS storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

Correct Answer: A

Reference:

<https://aws.amazon.com/storagegateway/file/>

Question #109

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon S3.

What should a solutions architect recommend to satisfy these requirements?

- A. Server-side encryption with customer-provided encryption keys
- B. Client-side encryption with Amazon S3 managed encryption keys
- C. Server-side encryption with keys stored in AWS Key Management Service (AWS KMS)
- D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Correct Answer: D

Question #110

A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted.

Which combination of steps will meet these requirements? (Choose two.)

- A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
- B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
- C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
- D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.
- E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the

S3 bucket so that only the newly created IAM role has read and download permissions.

Correct Answer: AB

Question #111

A company is investigating potential solutions that would collect, process, and store users' service usage data. The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure

Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.

Which solution should a solutions architect recommend?

- A. Use Amazon DynamoDB transactions.
- B. Create an Amazon Neptune database in a Multi-AZ design
- C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.
- D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon EBS Throughput Optimized HDD (st1) storage.

Correct Answer: C

Question #112

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.

How should a solutions architect optimize high availability for the application?

- A. Use Lambda@Edge for CloudFront.
- B. Use Amazon S3 Transfer Acceleration for CloudFront.
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Correct Answer: A

Question #113

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate AWS accounts. The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

Correct Answer: D

Question #114

A company currently stores symmetric encryption keys in a hardware security module (HSM). A solutions architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys.

Where should the key material be stored to meet these requirements?

- A. Amazon S3
- B. AWS Secrets Manager
- C. AWS Systems Manager Parameter store
- D. AWS Key Management Service (AWS KMS)

Correct Answer: D

Question #115

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Correct Answer: D

Question #116

A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.

Which solution should the solutions architect recommend?

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

Correct Answer: B

Question #117

A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet.

How should a solutions architect configure access?

- A. Create a private hosted zone using Amazon Route 53.
- B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
- C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.
- D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Correct Answer: B

Question #118

A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low latency.

Which architecture should a solutions architect recommend for this situation?

- A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.
- B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.
- C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
- D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

Correct Answer: D

Question #119

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: C

Question #120

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Correct Answer: D

Question #121

A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a

Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed.

Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency.

What should a solutions architect recommend as replacement database?

- A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
- B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
- D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Correct Answer: D

B

Question #122

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central

AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.

How should a solutions architect meet these requirements?

- A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.

- B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
- C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

Correct Answer: C B

Question #123

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environments and with AWS.

Which services meet the business requirements? (Choose two.)

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Correct Answer: CE

Question #124

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.

Which solution will accomplish this?

- A. Spot Fleet
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

Correct Answer: A

Question #125

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances.

What should a solutions architect do to accomplish this?

- A. Configure a volume using Amazon EFS. Mount the EFS volume to each Windows instance.
- B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.
- C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.
- D. Configure an Amazon EBS volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: C

Question #126

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.

What should a solutions architect do to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check.
- C. Create an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Correct Answer: C **B**

Question #127

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.

Which method should the solutions architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Correct Answer: A

Reference:

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-accelerator-dax-in-memory-caching-for-read-intensive-workloads/>

Question #128

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of

Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group.
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica.
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Correct Answer: C

Question #129

A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. The IAM policy must prevent function from performing any other actions on the Books table or any other.

Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        }  
    ]  
}
```

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"  
        }  
    ]  
}
```

C.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}

```

D.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        },
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Deny",
            "Action": "dynamodb:*:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}

```

Question #130

A

A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs.

What should a solutions architect do to reduce costs?

- A. Configure Amazon CloudFront with the existing website as the origin.
- B. Move the website to Amazon EC2 with Amazon EBS volumes for storage.
- C. Use AWS Global Accelerator and specify the existing website as the endpoint.
- D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Correct Answer: A

Question #131

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.

How should the company deploy this solution?

- A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
- B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
- D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Correct Answer: A

Question #132

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

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

Correct Answer: A D

Question #133

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 buckets it uses to store data. Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage.

Which solution will lower costs without compromising the availability of objects?

- A. Use S3 ACLs.
- B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.
- C. Use S3 Intelligent-Tiering storage.
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C

Question #134

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket. The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.

Which combination of actions should solutions archived take to accomplish this? (Choose two.)

- A. Create a VPC endpoint for Amazon S3.
- B. Enable server access logging on the bucket.
- C. Apply a bucket policy to restrict access to the S3 endpoint.
- D. Add an S3 ACL to the bucket that has sensitive information.
- E. Restrict users using the IAM policy to use the specific bucket.

Correct Answer: AC

Question #135

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.

How can a solutions architect make the system more responsive?

- A. Use Amazon SQS with AWS Lambda to generate reports.
- B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
- C. Update the client-side application code to increase its request timeout to 5 minutes.
- D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Correct Answer: A

Question #136

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.

What should the solutions architect do to meet these requirements?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Correct Answer: D

Question #137

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.

Which action will be MOST effective in accomplishing this?

- A. Replace the SQS queue with Amazon Kinesis Data Firehose.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
- D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Correct Answer: D

Question #138

A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads.

The application is critical to the business and must be highly available.

Which solution will meet these requirements?

- A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.
- B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.
- C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.
- D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

Correct Answer: C

A

Question #139

A solutions architect must design a solution for a persistent database that is being migrated from on-premises to AWS. The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.

Which solution effectively meets the database administrator's criteria?

- A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
- B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
- C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
- D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Correct Answer: B

Question #140

A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

- A. An Auto Scaling group with Spot Instance types.
- B. A placement group using a cluster placement strategy.
- C. A placement group using a partition placement strategy.
- D. An Auto Scaling group with On-Demand instance types.

Correct Answer: B

Question #141

A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.

What should a solutions architect recommend to reduce internet latency?

- A. Set up AWS Global Accelerator and add endpoints.
- B. Set up AWS Direct Connect locations in multiple Regions.
- C. Set up an Amazon CloudFront distribution to access an application.
- D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Correct Answer: A

Question #142

A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.

The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.

Which services satisfies these security requirements?

- A. AWS CloudHSM with the CloudHSM client
- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Correct Answer: A

Question #143

A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.

Which solution meets these requirements?

- A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

Correct Answer: A

Question #144

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances. The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests. Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A

Question #145

A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost-effective.

Which combination of AWS services and features should the solutions architect use? (Choose two.)

- A. Amazon S3
- B. Amazon EC2
- C. AWS Fargate
- D. Amazon CloudFront
- E. Elastic Load Balancer

Correct Answer: AD

Question #146

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

- A. Amazon EBS

- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Correct Answer: C

Question #147

A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The

Recovery Point Objective (RPO) must be less than 5 hours.

Which solutions can accomplish this? (Choose two.)

- A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
- B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
- C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
- D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
- E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

Correct Answer: AB **AE**

Question #148

A company has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-1 Region. A solutions architect is designing a disaster recovery strategy to have the database provisioned in the us-west-2 Region in case the database becomes unavailable in the us-east-1

Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

- A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.
- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
- D. Create a multimaster read/write instances across multiple AWS Regions. Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Correct Answer: B **A**

Question #149

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.

What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Correct Answer: A

Question #150

A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center.

The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.

What should the solutions architect do to meet these requirements?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS)
- C. Set up AWS Storage Gateway as a volume gateway
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: A

Question #151

A solutions architect is designing a hybrid application using the AWS cloud. The network between the on-premises data center and AWS will use an AWS Direct

Connect (DX) connection. The application connectivity between AWS and the on-premises data center must be highly resilient.

Which DX configuration should be implemented to meet these requirements?

- A. Configure a DX connection with a VPN on top of it.
- B. Configure DX connections at multiple DX locations.
- C. Configure a DX connection using the most reliable DX partner.
- D. Configure multiple virtual interfaces on top of a DX connection.

Correct Answer: B

Question #152

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.

Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

- A. Deploy a NAT instance in a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Correct Answer: B

Question #153

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon

RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running.

The business reporting users must be able to generate reports without affecting the application's performance.

Which action will accomplish this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Correct Answer: D

Question #154

A company is running a two-tier ecommerce website using services. The current architect uses a publish-facing Elastic Load Balancer that sends traffic to Amazon

EC2 instances in a private subnet. The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database.

The application is running in the United States. The company recently started selling to users in Europe and Australia. A solutions architect needs to design solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances.

D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Correct Answer: B

Question #155

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A

Question #156

A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server databases running on Amazon EC2 instances with

Windows Server 2016. The solution must be able to be integrated into the corporate Active Directory domain, be highly durable, be managed by AWS, and provide high levels of throughput and IOPS.

Which solution meets these requirements?

- A. Use Amazon FSx for Windows File Server.
- B. Use Amazon Elastic File System (Amazon EFS).
- C. Use AWS Storage Gateway in file gateway mode.
- D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Correct Answer: A

Question #157

A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions. The company wants to create an allow list for the IPs of all the load balancers on its firewall device. A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall.

What should the solutions architect recommend to meet these requirements?

- A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IPs. Register the private IPs of all the ALBs as targets to this NLB.
- C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.

D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

Correct Answer: C

Question #158

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B

Question #159

A company is planning to migrate its virtual server-based workloads to AWS. The company has internet-facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository.

Which services should a solutions architect recommend be hosted on the public subnet? (Choose two.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Correct Answer: AC

Question #160

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Correct Answer: B

Question #161

A company is using a tape backup solution to store its key application data offsite. The daily data volume is around 50 TB. The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed, and a week's notice is typically given if a backup needs to be restored.

The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes. The company also wants to make sure that the transition from tape backups to the cloud minimizes disruptions.

Which storage solution is MOST cost-effective?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

Correct Answer: A

Question #162

A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead.

Which solution should the solutions architect implement?

- A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.
- B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
- C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
- D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Correct Answer: A

Question #163

A company decides to migrate its three-tier web application from on-premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.

Which AWS service meets these requirements?

- A. Amazon Aurora
- B. Amazon RDS for SqlServer
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB on-demand

Correct Answer: A

Question #164

A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.

Which method should a solutions architect implement to meet this requirement?

- A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs.
- B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs.
- C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs.
- D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

Correct Answer: D

Question #165

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross-communication. A recent increase in account creations and

VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally managed networking setup for multiple accounts, VPCs, and VPNs.

Which networking solution meets these requirements?

- A. Configure shared VPCs and VPNs and share to each other.
- B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect connection between all VPCs and VPNs.
- D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

Correct Answer: D

Question #166

A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.

Which database solution meets these requirements?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Correct Answer: B

Question #167

A solutions architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architected has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file Share to Amazon RDS.
- B. Migrate the file Share to AWS Storage Gateway
- C. Migrate the file Share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Correct Answer: C

Question #168

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Correct Answer: A

Question #169

A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.

If an Availability Zone fails, how can the company remain compliant with the SLA?

- A. Add a target tracking scaling policy with a short cooldown period.
- B. Change the Auto Scaling group launch configuration to use a larger instance type.
- C. Change the Auto Scaling group to use six servers across three Availability Zones.
- D. Change the Auto Scaling group to use eight servers across two Availability Zones.

Correct Answer: A C

Question #170

A company is reviewing its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization. A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

- A. Enable AWS Config service with the appropriate rules
- B. Enable AWS Trusted Advisor with the appropriate checks.
- C. Write a script using an AWS SDK to generate a bucket report
- D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Correct Answer: A

Question #171

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency.

What should a solutions architect recommend to meet these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.
- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Correct Answer: B

Question #172

A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain.

Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).
- B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure

SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.

D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

Correct Answer: D C

Question #173

A solutions architect has configured the following IAM policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "lambda:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "lambda:CreateFunction",  
                "lambda>DeleteFunction"  
            ],  
            "Resource": "*"  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "220.100.16.0/20"  
                }  
            }  
        }  
    ]  
}
```

Which action will be allowed by the policy?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

Correct Answer: C

Question #174

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an

Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

- A. S3 Standard

- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B

Question #175

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

- A. Move static assets to Amazon CloudFront. Leave the application in EC2 in an Auto Scaling group. Move the database to Amazon RDS to deploy Multi-AZ.
- B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.
- C. Move static assets to Amazon S3. Move the application to AWS Lambda with the concurrency limit set. Move the database to Amazon DynamoDB with on-demand enabled.
- D. Move static assets to Amazon S3. Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled. Move the database to Amazon RDS to deploy Multi-AZ.

Correct Answer: B D

Question #176

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content. This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

- A. Change the EBS volume to Provisioned IOPS (PIOPS).
- B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.
- C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.
- D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Correct Answer: B

Question #177

A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

- A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.
- B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
- D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
- E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Correct Answer: AC AB

Question #178

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists. The company is looking for a native, software-based AWS service to accomplish this goal.

What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Correct Answer: A B

Question #179

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

Correct Answer: C

Question #180

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Correct Answer: B

Question #181

A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and

JavaScript.

Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Choose two.)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Correct Answer: DE

Question #182

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only.

What should a solutions architect do to protect against data loss? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.

E. Use MFA Delete to require multi-factor authentication to delete an object.

Correct Answer: AE

Question #183

An operations team has a standard that states IAM policies should not be applied directly to users. Some new team members have not been following this standard. The operations manager needs a way to easily identify the users with attached policies.

What should a solutions architect do to accomplish this?

- A. Monitor using AWS CloudTrail.
- B. Create an AWS Config rule to run daily.
- C. Publish IAM user changes to Amazon SNS.
- D. Run AWS Lambda when a user is modified.

Correct Answer: C B

Question #184

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.

Which solution should the solutions architect select?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Correct Answer: C

Question #185

A company is building applications in containers. The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS. Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software. Which solution meets these requirements?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.
- C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

Correct Answer: B

Question #186

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling. Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy.

Correct Answer: C D

Question #187

A solutions architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The solutions architect must improve the security posture and minimize the impact of a DDoS attack on resources.

Which solution is MOST effective?

- A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.
- B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
- C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda function that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
- D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

Correct Answer: B A

Question #188

A company has multiple AWS accounts for various departments. One of the departments wants to share an Amazon S3 bucket with all other departments.

Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket.
- B. Create a pre-signed URL for the bucket and share it with other departments.

- C. Set the S3 bucket policy to allow cross-account access to other departments.
- D. Create IAM users for each of the departments and configure a read-only IAM policy.

Correct Answer: C

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

Question #189

A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects. Which action should be taken to share the S3 bucket?

- A. Update the bucket to be a Requester Pays bucket.
- B. Update the bucket to enable cross-origin resource sharing (CORS).
- C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.
- D. Create an IAM policy to require users to grant bucket-owner-full-control when uploading objects.

Correct Answer: C

By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. To get access to the object, the object owner must explicitly grant you (the bucket owner) access. The object owner can grant the bucket owner full control of the object by updating the access control list (ACL) of the object. The object owner can update the ACL either during a put or copy operation, or after the object is added to the bucket.

Similar:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-require-object-ownership/>

Resolution Add a bucket policy that grants users access to put objects in your bucket only when they grant you (the bucket owner) full control of the object.

Reference:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-bucket-owner-access/>

Question #190

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention. Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Correct Answer: B

Question #191

A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.

What is the FASTEST way to aggregate data from all of these global sites?

- A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
- B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon EBS volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

Correct Answer: A

Step-1: To transfer to S3 from global sites: Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's™ globally distributed AWS Edge Locations. Used to accelerate object uploads to S3 over long distances (latency). Transfer acceleration is as secure as a direct upload to S3.

Step-2: When the application analyzes/aggregates the data from S3 and then again uploads the results - Multipart upload

Reference:

<http://lavnish.blogspot.com/2017/06/aws-s3-cross-region-replication.html> <https://aws.amazon.com/s3/transfer-acceleration/>

Question #192

A company has a custom application running on an Amazon EC2 instance that:

- ↳ Reads a large amount of data from Amazon S3
- ↳ Performs a multi-stage analysis
- ↳ Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis. The process performance depends on the temporary storage performance.

What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Correct Answer: A

D

Question #193

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers

can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Correct Answer: **B** D

Question #194

A company recently released a new type of internet-connected sensor. The company is expecting to sell thousands of sensors, which are designed to stream high volumes of data each second to a central location. A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness.

Which solution should the solutions architect recommend?

- A. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- B. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
- C. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Correct Answer: **D**

Question #195

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.

How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Correct Answer: D C

Question #196

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Correct Answer: C

Question #197

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Correct Answer: B C

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

Question #198

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

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

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

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

Correct Answer: AE

Question #199

A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for a minimum of two instances and a maximum of four instances across two Availability Zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for all the EC2 instances.

What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

- A. Remove some EC2 instances to increase the utilization of remaining instances.
- B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
- C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
- D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

D

Amazon AWS Certified Solutions Architect - Associate SAA-C02

Question #200

A company has an application that posts messages to Amazon SQS. Another application polls the queue and processes the messages in an I/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages, the company has difficulty meeting its SLA consistently.

What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

- A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.
- B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance.
- C. Create an Amazon Machine image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy to keep its aggregate CPU utilization below 70%.
- D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

D

Question #201

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.

- B. An Application Load Balancer with an associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

A

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/>

Question #202

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

B

Anything that says something like "..deploy database to an instance.." is not highly scaleable. The best way to take advantage of the available AWS services for databases.

Question #203

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to further reduce data transfer costs. The company cannot modify the application's source code. What should a solutions architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users

A

Use Lambda@Edge. See the question "single-use text file" will be sent in response. Single-use text file means that file will be used only one time so what's the benefit of caching it on the CloudFront as it will not be able to be used again. So what other thing can be done is to use Lambda@Edge to compress the file which will reduce the size of the file and hence less data will be transferred and less will be the transfer charges.

Question #204

A database is on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that experiences highly dynamic reads. Application developers notice a significant slowdown when testing read performance from a secondary AWS Region. The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

- A. Install MySQL on Amazon EC2 in the secondary Region.
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary Region.
- D. Implement Amazon ElastiCache to improve database query performance.

B

As an alternative to cross-Region read replicas, you can scale read operations with minimal lagtime by using an Aurora global database. An Aurora global database has a primary Aurora DB cluster in one AWS Region and up to five secondary read-only DB clusters in different Regions. Each secondary DB cluster can include up to 16 (rather than 15) Aurora Replicas. Replication from the primary DB cluster to all

secondaries is handled by the Aurora storage layer rather than by the database engine, so lagtime for replicating changes is minimal—typically, less than 1 second.

Question #205

A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days. Which solution should a solutions architect recommend?

- A. Set the backup retention period to 90 days when creating the RDS DB instance.
- B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.
- C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days. Create an AWS Backup job to schedule the execution of the backup plan daily.
- D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot. Purge snapshots older than 90 days.

C

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html>

Question #206

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation.

What should a solutions architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.

C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.

D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

D A

<https://aws.amazon.com/s3/features/batch-operations/>

Data is already in S3. Snowball is to transfer data from data center to AWS. Hence B & C are wrong. Lambda doesn't let you install custom software. So batch processing on S3 is not possible. As question asked to minimize the data transfer cost. D makes sense as you install EC2 in same region as S3

Question #207

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority. Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

A

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html>

Question #208

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

D

Microsoft Windows shared file storage => FSx

Question #209

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications. Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

C

<https://aws.amazon.com/rds/aurora/serverless/>

Question #210

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

A

Question #211

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

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

C

<https://aws.amazon.com/ec2/pricing/on-demand/>

Question #212

A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.

What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

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

D

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.

<https://aws.amazon.com/transit-gateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Question #213

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users. What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.

- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

B

- Changing IP addr, cannot be NACL
- AWS inspector assesses applications for exposure, vulnerabilities, and deviations from best practices, so it's for penetration tests and so on
- AWS GuradDuty, threat detection not prevention

Question #214

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.

What should the solutions architect recommend to build the MOST high-performing solution?

- A. Use AWS Glue to process data and Amazon S3 to store data.
- B. Use Amazon EMR to process data and Amazon Redshift to store data.
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

B

Question #215

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database.

The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

- A. Launch an Amazon ElastiCache cluster to cache common database queries.
- B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
- C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.
- D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

B

Question #216

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends. A solutions architect needs to design a cost-effective solution that can handle the load.

What should the solutions architect do to meet these requirements?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable Multi-AZ replication for the DynamoDB database.
- C. Enable DynamoDB auto scaling when creating the tables.
- D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

C

DynamoDB modes: On-demand – unknown workloads Provisioned – predictable application traffic
<https://aws.amazon.com/dynamodb/pricing/>

Question #217

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

- A. Enable concurrency scaling.
- B. Enable cross-Region snapshots.
- C. Increase the data retention period.
- D. Deploy Amazon Redshift in Multi-AZ.

B

<https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/>

A - NO - because it's about performance

C - NO - there is no option to do this

D - NO - cause each cluster is independent

Question #218

A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

- A. Amazon Redshift
- B. AWS Storage Gateway for files
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

B

use case for file gateway: "Hybrid cloud workflows using data generated by on-premises applications for processing by AWS services such as machine learning, big data analytics or serverless functions."

Question #219

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

D

"You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, Amazon API Gateway for your REST APIs, or AWS AppSync for your GraphQL APIs. With AWS WAF, you pay only for what you use and the pricing is based on how many rules you deploy and how many web requests your application receives".

Question #220

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company's needs and takes the LEAST amount of time?

- A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.

- B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.
- C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.
- D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora

D

100mbps will take 143 days.

500mbps will need to be ordered, then it'll take another 25 days.

Snowmobile is an overkill.

50 TB Snowballs have 42 TB of usable space. so $42 \times 3 = 126$ (less than 143TB) so they need to order 4 snowballs(168TB).

<https://docs.aws.amazon.com/snowball/latest/ug/specifications.html>

Question #221

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

A

<https://aws.amazon.com/rds/features/multi-az/>

To convert an existing Single-AZ DB Instance to a Multi-AZ deployment, use the "Modify" option corresponding to your DB Instance in the AWS Management Console.

Question #222

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum. What should a solutions architect recommend?

- A. Set up a new Direct Connect connection in another AWS Region.
- B. Set up a new AWS managed VPN connection in another AWS Region.
- C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
- D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

C

<https://aws.amazon.com/directconnect/resiliency-recommendation/>

Question #223

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

A

- 1. NAT Gateways = connect Private Subnets to the Internet
- 2. NAT gateways = Highly available
- 3. NAT Gateway = a highly available AWS managed service that makes it easy to connect to the Internet from instances within a private subnet in an Amazon Virtual Private Cloud (Amazon VPC). Previously, you needed to launch a NAT instance to enable NAT for instances in a private subnet.

Question #224

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

B

The "management" is the keyword. You don't give your boss details, it will only confuse them.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-reports.html>

Question #225

A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.

What should a solutions architect recommend?

- A. Use Amazon DynamoDB global tables.
- B. Use Amazon Aurora Global Database.
- C. Use Amazon RDS for MySQL with a cross-Region read replica.
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

B

<https://medium.com/capital-one-tech/moving-to-dynamodb-to-increase-application-resiliency-106d753d38b1>

Question #226

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

A E

There are 2 ingestion and 3 processor Since the near real-time we choose Firehose - A - First step We are left with processor, B , D and E We know lambda can run max for 15 min and the job is of 30 min so lambda is out.

<https://aws.amazon.com/lambda/faqs/#:~:text=AWS%20Lambda%20functions%20can%20be,1%20second%20and%2015%20minutes>. We are left with D and E Both will work but the question specifies serverless hence E - step 2 <https://aws.amazon.com/fargate/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc&fargate-blogs.sort-by=item.additionalFields.createdDate&fargate-blogs.sort-order=desc>

Question #227

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.

Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

- A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
- B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
- C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
- D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Question #228

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored. The amount of

data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1 TB. Which storage solution should the solutions architect recommend?

- A. An Amazon DynamoDB table accessible by all ECS cluster instances.
- B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
- C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
- D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

B

Size (1TB=1000GB) is not enough to cover throughput requirement: @50 KB/s per GB of throughput in burst mode --> $50 * 1000\text{GB} = 50000\text{KB/s} = 50\text{MB/s}$ while you have to manage an "amount of data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time" --> $10\text{MB} * 200\text{ ("hundreds")} = 2000\text{MB}$ which looks like another order of magnitude... ok you can burst, but doesn't look stable. There are no cost restriction mentioned therefore B is the way to go, provisioned throughput (BTW just the fact that you have an idea of the throughput should suggest to go provisioned).

Question #229

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.

Which configuration should a solutions architect recommend?

- A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.
- B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.
- C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.

- D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

C

<https://aws.amazon.com/sqs/features/>

Question #230

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

B

- A. Sounds wrong, you'll have to enable Multi-AZ deployment.
- B. Sounds about right.
- C. Read replicas don't help or make the DB reliable.
- D. Nop, EC2 is not recommended.

Question #231

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

Which storage solution meets these requirements?

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

B

Intelligent tiering moves data between storage classes based on its current degree of usage.

Question #232

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

- A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.

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

A

- A. Sounds like a good option, except it will take longer than B.
- B. Could work with a CloudFormation template but why only an Application Load Balancer, where is the Auto Scaling group? But it's being executed from a script... not sure if that sounds right, since if the data center fails... you won't be able to execute the script.
- C. Sounds a lot of work just to create an Application Load Balancer. And we also need to backup volumes.
- D. A lot of things to setup, Direct Connect will take a long time already.

Question #233

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

A

<https://aws.amazon.com/premiumsupport/knowledge-center/transit-gateway-connect-vpcs-from-vpn/>

Question #234

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

D

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#:~:text=Solution%20overview,console%2C%20CLI%2C%20or%20SDK.&text=To%20encrypt%20an%20object%20at,S3%2C%20or%20SSE%2DKMS>

Question #235

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.

What is the MOST cost-effective method to establish this type of connection?

- A. Implement a client VPN.
- B. Implement AWS Direct Connect.
- C. Implement a bastion host on Amazon EC2.
- D. Implement an AWS Site-to-Site VPN connection.

D

A. Incorrect - AWS Client VPN is an AWS managed high availability and scalability service enabling secure software remote access. It provides the option of creating a secure TLS connection between remote clients and your Amazon VPCs, to securely access AWS resources and on-premises over the internet, Refer - <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-client-vpn.html>

D is correct here AWS site to site VPN is applicable to make the line secure and to allow access to all AWS/Network resources

Question #236

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year.

The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

- A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
- B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
- C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
- D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

C

<https://aws.amazon.com/global-accelerator/faqs/>

: "Associate the static IP addresses provided by AWS Global Accelerator to regional AWS resources or endpoints, such as Network Load Balancers, Application Load Balancers, EC2 Instances, and Elastic IP addresses"

Question #237

A company runs a high performance computing (HPC) workload on AWS. The workload required low-latency network performance and high network throughput with tightly coupled

node-to-node communication. The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.

What should a solutions architect propose to improve the performance of the workload?

- A. Choose a cluster placement group while launching Amazon EC2 instances.
- B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
- C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
- D. Choose the required capacity reservation while launching Amazon EC2 instances.

A

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-placementgroup.html>

: "A cluster placement group is a logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput"

Question #238

A company uses a legacy on-premises analytics application that operates on gigabytes of .csv files and represents months of data. The legacy application cannot handle the growing size of .csv files. New .csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services. To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solutions architect recommend?

- A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company's on-premises storage and the company's S3 bucket.
- B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.
- C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.

D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon EFS to the company's S3 bucket.

A

<https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Question #239

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.
What should a solutions architect recommend?

- A. Set up a corporate Amazon S3 bucket and move all media and application files.
- B. Configure Amazon FSx for Windows File Server and move all the media and application files.
- C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
- D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

B

<https://aws.amazon.com/fsx/windows/>

It says that the files need to be shared internally, and it's using Active Directory. Amazon FSX for Windows sounds about right. (B).

Question #240

A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the VPC was designed with two public

subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances. What should a solutions architect do to ensure these requirements are met?

- A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.
- C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

C

since Internet-facing Application Load Balancers (ALB) and Classic ELBs must be provisioned exclusively in public subnets.

Question #241

A company is experiencing growth as demand for its product has increased. The company's existing purchasing application is slow when traffic spikes. The application is a monolithic three-tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier. A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes.

Which solution will meet these requirements?

- A. Vertically scale the application instance using a larger Amazon EC2 instance size.
- B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS.
- C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.
- D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

C

Question #242

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

B

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-event-notifications.html>

Question #243

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use of AWS Snowball.

What should a solutions architect recommend to accomplish this?

- A. Order a Snowball Edge device to copy the data from one Region to another Region.
- B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
- C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.

- D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

c D

<https://aws.amazon.com/premiumsupport/knowledge-center/move-objects-s3-bucket/>

Question #244

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

B

https://aws.amazon.com/redshift/features/?nc=sn&loc=2&dn=1&refid=ps_a134p000007banyaas&trk_campaign=acq_paid_search_brand

Question #245

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.

What should a solutions architect recommend?

- A. Use an Auto Scaling group with a cluster placement group.

- B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
- C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
- D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Question #246

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

A

last line of the question that says " The company also wants to minimize the management overhead required to maintain the solution." : That means "Serverless Technologies" and except A in all three other options there are EC2 involved ,which needs lot of maintenance !!!!

Question #247

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement. What should a solutions architect recommend?

- A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
- B. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.
- C. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
- D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

B

Question #248

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

A.

```

    "Action": [
        "s3:*Object"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"
B.
    "Action": [
        "s3:*
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"
C.
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"
D.
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"

```

D

Question #249

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified. Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.

C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.

D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

Question #250

A company wants to share forensic accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and requires its own copy of the database.

How should the company securely share the database with the auditor?

A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.

B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.

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

D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

D

A. The question says the auditor needs its own copy of the database. A read replica won't do this request.

B. We can't have direct access to the bucket in S3.

C. Sounds a lot of work, I doubt, someone is going to be auditing from text files.

D. Sounds reasonable. Making an encrypted snapshot, the auditor, will have its own copy of the database.

Question #251

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

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

B

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

Question #252

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.

The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.

- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

B

<https://www.youtube.com/watch?app=desktop&v=s0XFX3WHg0w>

Question #253

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

B

Api Gateway is scalable, and elastic, same as Lambda

Question #254

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

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

B

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

<https://aws.amazon.com/ebs/features/>

Question #255

A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access. The application will use Amazon EC2 instances with a user data script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost?

- A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.
- B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.
- C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.

D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

D

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

Question #256

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBC snapshots are encrypted.

What should the solutions architect do to accomplish this?

- A. Enable EBS encryption by default for the AWS Region.
- B. Enable EBS encryption by default for the specific volumes.
- C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.
- D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption

A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#volume-account-on>

Question #257

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.

What should a solutions architect recommend to meet these requirements?

- A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
- B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.

C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.

D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

A

<https://aws.amazon.com/cloudfront/faqs/>

Question #258

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

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

A.

Job can be started and stopped at any given time with no negative impact. Perfect scenario.

Question #259

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce costs.

What should a solutions architect recommend?

- A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.

- B. Implement CloudFront events with Lambda@Edge to run the website's data processing.
- C. Modify the CloudFront price class to include only the locations of the countries that are served.
- D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PriceClass.html>

Question #260

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

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

A

dedicated-hosts = visibility of sockets and physical cores

Question #261

A company is designing a website that uses an Amazon S3 bucket to store static images. The company wants all future requests to have faster response times while reducing both latency and cost.

Which service configuration should a solutions architect recommend?

- A. Deploy a NAT server in front of Amazon S3.
- B. Deploy Amazon CloudFront in front of Amazon S3.
- C. Deploy a Network Load Balancer in front of Amazon S3.
- D. Configure Auto Scaling to automatically adjust the capacity of the website.

B

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

Question #262

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

B

<https://aws.amazon.com/rds/aurora/mysql-features/>

Question #263

A company needs to comply with a regulatory requirement that states all emails must be stored and archived externally for 7 years. An administrator has created compressed email files on premises and wants a managed service to transfer the files to AWS storage.

Which managed service should a solutions architect recommend?

- A. Amazon Elastic File System (Amazon EFS)

- B. Amazon S3 Glacier
- C. AWS Backup
- D. AWS Storage Gateway

D

<https://aws.amazon.com/storagegateway/faqs/>

Question #264

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named CompanyConfidential. The cloud engineer must be able to read from and write to an S3 bucket called AdminTools.

Which IAM policy will meet these requirements?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": "arn:aws:s3:::AdminTools"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

B.

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListBucket",
            "Resource": [
                "arn:aws:s3:::AdminTools",
                "arn:aws:s3:::CompanyConfidential/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::CompanyConfidential"
        }
    ]
}
C.
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject" ],
            "Resource": "arn:aws:s3:::AdminTools/*",
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::CompanyConfidential"
            ]
        }
    ]
}

```

D.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListBucket",
            "Resource": "arn:aws:s3:::AdminTools/*"
        },
        {
            "Effect": "Allow",
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],
            "Resource": "arn:aws:s3:::AdminTools/"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::CompanyConfidential",
                "arn:aws:s3:::CompanyConfidential/*",
                "arn:aws:s3:::AdminTools/*"
            ]
        }
    ]
}
```

A

<https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/>

Question #265

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

A

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html>

Question #266

A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS.

Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.

The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.

Which solution meets these requirements?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
- B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

B.

EC2 cannot be correct as question states "no server maintenance"

Question #267

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Choose two.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53.
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

DE

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html

Question #268

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.

What should a solutions architect do to minimize the anticipated server load?

- A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.
- B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
- C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
- D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

Question #269

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.

Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

Question #270

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solutions architect recommend to provide a highly available and scalable solution?

- A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
- B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
- C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.
- D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

A

Question #271

Management has decided to deploy all AWS VPCs with IPv6 enabled. After some time, a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet.

What should the solutions architect do to fix this?

- A. Check to make sure that only IPv6 was used during the VPC creation.
- B. Create a new IPv4 subnet with a larger range, and then launch the instance.
- C. Create a new IPv6-only subnet with a large range, and then launch the instance.
- D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

B

Question #272

A company has a build server that is in an Auto Scaling group and often has multiple Linux instances running. The build server requires consistent and mountable shared NFS storage for jobs and configurations.

Which storage option should a solutions architect recommend?

- A. Amazon S3
- B. Amazon FSx
- C. Amazon Elastic Block Store (Amazon EBS)

D. Amazon Elastic File System (Amazon EFS)

D

Question #273

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a

NAT instance for internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

- A. Configure a NAT gateway to replace the NAT instances.
- B. Configure a gateway endpoint for traffic destined to Amazon S3.
- C. Configure an interface endpoint for traffic destined to Amazon S3.
- D. Configure Amazon CloudFront for the S3 bucket storing the images.

B

Question #274

The financial application at a company stores monthly reports in an Amazon S3 bucket. The vice president of finance has mandated that all access to these reports be logged and that any modifications to the log files be detected.

Which actions can a solutions architect take to meet these requirements?

- A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled.
- B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled.
- C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.
- D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

C

Question #275

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and

configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.

D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

D

Question #276

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company's account. All the needed policies have been created to grant appropriate access.

Which additional component will provide the vendor with the MOST secure access to the account?

- A. Create an IAM user.
- B. Implement a service control policy (SCP)
- C. Use a cross-account role with an external ID.
- D. Configure a single sign-on (SSO) identity provider.

C

Question #277

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

AD

Question #278

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS.

However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.
- C. Build a database cache using Amazon ElastiCache.
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

C

Question #279

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices.

The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.
- B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

D

Question #280

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users.

During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

D

Question #281

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the

virtual private gateway.

B

Question #282

A company is backing up on-premises databases to local file server shares using the SMB protocol. The company requires immediate access to 1 week of backup files to meet recovery objectives. Recovery after a week is less likely to occur, and the company can tolerate a delay in accessing those older backup files.

What should a solutions architect do to meet these requirements with the LEAST operational effort?

- A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.
- B. Deploy an AWS Storage Gateway file gateway with sufficient storage to hold 1 week of backups. Point the backups to SMB shares from the file gateway.
- C. Deploy Amazon Elastic File System (Amazon EFS) to create a file system with exposed NFS shares with sufficient storage to hold all the desired backups.
- D. Continue to back up to the existing file shares. Deploy AWS Database Migration Service (AWS DMS) and define a copy task to copy backup files older than 1 week to Amazon S3, and delete the backup files from the local file store.

B

Question #283

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon

EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a period of time during surges. A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

D

Question #284

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solution architect needs to bring that data on premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.
- D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Question #285

D

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

A

Question #286

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

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

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

B

Question #287

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be executed when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be executed when needed. Configure the

DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.

D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

A

Question #288

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

B

Question #289

A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled. For compliance reasons, the older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.

What should the solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use S3 batch operations to replace object tags. Expire the objects based on the modified tags.
- B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.
- C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SQS) queue for further processing.
- D. Replicate older object versions to a new bucket. Use an S3 Lifecycle policy to expire the objects in the new bucket after 2 years.

B

Question #290

A company runs an application on an Amazon EC2 instance backed by Amazon Elastic Block Store (Amazon EBS). The instance needs to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application. However, the contents of the instance's memory must be preserved whenever the instance is unavailable.

What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
- D. Terminate the instance outside the application's availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

B

Question #291

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from

0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

C

Question #292

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by a way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

B

Question #293

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

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

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

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

D

Question #294

A company is moving its on-premises applications to Amazon EC2 instances. However, as a result of fluctuating compute requirements, the EC2 instances must always be ready to use between 8 AM and 5 PM in specific Availability Zones.

Which EC2 instances should the company choose to run the applications?

- A. Scheduled Reserved Instances
- B. On-Demand Instances
- C. Spot Instances as part of a Spot Fleet
- D. EC2 instances in an Auto Scaling group

D

Question #295

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

D

Question #296

A company is building an application on Amazon EC2 instances that generates temporary transactional data. The application requires access to data storage that can provide configurable and consistent IOPS.

What should a solutions architect recommend?

- A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
- B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
- C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.
- D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

C

Question #297

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.

Which storage solution meets these requirements?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

B

Question #298

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

A

Question #299

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting high request latency for users located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

How should a solutions architect accomplish this?

- A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
- C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway

stage to enable the API cache.

D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

B

Question #300

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users. The service is hosted in a VPC behind a

Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.

What should a solutions architect do to accomplish this goal?

- A. Create a peering VPC connection from each user's VPC to the software vendor's VPC.
- B. Deploy a transit VPC in the software vendor's AWS account. Create a VPN connection with each user account.
- C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.
- D. Deploy a transit VPC in the software vendor's AWS account. Create an AWS Direct Connect connection with each user account.

C

Question #301

A user wants to list the IAM role that is attached to their Amazon EC2 instance. The user has login access to the EC2 instance but does not have IAM permissions.

What should a solutions architect do to retrieve this information?

- A. Run the following EC2 command: curl http://169.254.169.254/latest/meta-data/iam/info
- B. Run the following EC2 command: curl http://169.254.169.254/latest/user-data/iam/info
- C. Run the following EC2 command: http://169.254.169.254/latest/dynamic/instance-identity/
- D. Run the following AWS CLI command: aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

A

Question #302

A company has an application that is hosted on Amazon EC2 instances in two private subnets. A solutions architect must make the application available on the public internet with the least amount of administrative effort.

What should the solutions architect recommend?

- A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.
- D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and

associate two private subnets from the same Availability Zones as the public instances.

A

Question #303

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

C

Question #304

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

A

Question #305

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

What should the solutions architect do to meet this requirement?

- A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.
- B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
- C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.

D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

B

Question #306

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL. In the database layer several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

B

Question #307

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

C

Question #308

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.

C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.

D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

D

Question #309

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.

The following are the key requirements:

- The web servers must be accessible only to users on an SSL connection.
- The database should be accessible to the web layer, which is created in a public subnet only.
- All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Select two.)

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0).
- B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
- C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.
- E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

BD

Question #310

A company has an on-premises application that collects data and stores it to an on-premises NFS server. The company recently set up a 10 Gbps AWS Direct Connect connection. The company is running out of storage capacity on premises. The company needs to migrate the application data from on-premises to the AWS Cloud while maintaining low-latency access to the data from the on-premises application.

What should a solutions architect do to meet these requirements?

- A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.
- C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

D

Question #311

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement and support the NFS protocol.

Which solution meets these requirements?

- A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
- B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the Instances and apply that to the additional instance.
- C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 Instances that need access to the data.
- D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

A

Question #312

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability. The company wants to be able to deploy updates to its application even if nodes in one Availability Zone are not accessible.

The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to

100%.

Which configuration of tasks and Availability Zones meets these requirements?

- A. Deploy the application across two Availability Zones, with one task in each Availability Zone.
- B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
- C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
- D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

D

Question #313

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

A

Question #314

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on

Amazon EC2 instances in different AWS Regions and a stateless UDP-based workload hosted on premises.

Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

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

AD

Question #315

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand

Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day.

An Application

Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

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

A

Question #316

A company has an ecommerce application running in a single VPC. The application stack has a single web server and an Amazon RDS Multi-AZ DB instance.

The company launches new products twice a month. This increases website traffic by approximately 400% for a minimum of 72 hours. During product launches, users experience slow response times and frequent timeout errors in their browsers.

What should a solutions architect do to mitigate the slow response times and timeout errors while minimizing operational overhead?

- A. Increase the instance size of the web server.
- B. Add an Application Load Balancer and an additional web server.
- C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.

D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

C

Question #317

A solutions architect is designing an architecture to run a third-party database server. The database software is memory intensive and has a CPU-based licensing model where the cost increases with the number of vCPU cores within the operating system. The solutions architect must select an Amazon EC2 instance with sufficient memory to run the database software, but the selected instance has a large number of vCPUs. The solutions architect must ensure that the vCPUs will not be underutilized and must minimize costs.

Which solution meets these requirements?

- A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.
- B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.
- C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.
- D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

B

Question #318

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

B

Question #319

A company is creating a web application that will store a large number of images in Amazon S3. The images will be accessed by users over variable periods of time. The company wants to:

- Retain all the images
- Incur no cost for retrieval.
- Have minimal management overhead.
- Have the images available with no impact on retrieval time.

Which solution meets these requirements?

- A. Implement S3 Intelligent-Tiering
- B. Implement S3 storage class analysis
- C. Implement an S3 Lifecycle policy to move data to S3 Standard-Infrequent Access (S3 Standard-IA).

D. Implement an S3 Lifecycle policy to move data to S3 One Zone-Infrequent Access (S3 One Zone-IA).

A

Question #320

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

D

Question #321

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order, two microservices should handle the event simultaneously. The Email microservice will send a confirmation email, and the OrderProcessing microservice will start the order delivery process. If a customer cancels an order, the OrderCancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

- A. Create a single SQS queue and publish order events to it. The Email OrderProcessing and Order Cancellation microservices can then consume messages of the queue.
- B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email OrderProcessing and Order Cancellation microservices to its own topic.
- C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email OrderProcessing and Order Cancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.
- D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and Order Cancellation microservices.

C

Question #322

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL

Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon EBS General Purpose SSD (gp2) volume. The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the

number of read and write IOPS is higher than 6,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a Magnetic volume.
- B. Increase the number of IOPS on the gp2 volume.
- C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
- D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

C

Question #323

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is shared across a cluster of Linux servers. The company wants to reduce storage costs for the application.

What should a solutions architect do to meet these requirements?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon EFS and store them locally on each Amazon EC2 instance.
- C. Configure a Lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
- D. Move the files to Amazon S3 with S3 lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

C

Question #324

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solution architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

A

Question #325

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

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

D

Question #326

A company wants to migrate its web application to AWS. The legacy web application consists of a web tier, an application tier, and a MySQL database. The re-architected application must consist of technologies that do not require the administration team to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Choose two.)

- A. Amazon Aurora Serverless
- B. Amazon EC2 Spot Instances
- C. Amazon Elasticsearch Service (Amazon ES)
- D. Amazon RDS for MySQL
- E. AWS Fargate

AE

Question #327

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

B

Question #328

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.

D. Increase the Provisioned IOPS on the Aurora instance.

B

Question #329

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

BD

Question #330

A solution architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Amazon EC2 instances in private subnets Configure. Configure a public Application Load Balancer with multiple redundant Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

C

Question #331

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region it runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.

C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.

D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

A

Question #332

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in

Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.

B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.

C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.

D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

C

Question #333

A development team stores its Amazon RDS MySQL DB instance user name and password credentials in a configuration file. The configuration file is stored as plaintext on the root device volume of the team's Amazon EC2 instance. When the team's application needs to reach the database, it reads the file and loads the credentials into the code. The team has modified the permissions of the configuration file so that only the application can read its content. A solution architect must design a more secure solution.

What should the solutions architect do to meet this requirement?

A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.

B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.

C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.

D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

B

Question #334

A company wants a storage option that enables its data science team to analyze its data on premises and in the AWS Cloud. The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones. What should a solutions architect do to meet these requirements?

- A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
- B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
- C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

D

Question #335

A company wants to improve the availability and performance of its stateless UDP-based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions.

What should a solutions architect recommend to accomplish this?

- A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
- B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.
- C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
- D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

A

Question #336

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each

HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

A

Question #337

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead from aging and scaling the database must be minimized.

Which database solution should the solutions architect recommend?

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

A

Question #338

A company is working with an external vendor that requires write access to the company's Amazon Simple Queue Service (Amazon SQS) queue. The vendor has its own AWS account.

What should a solutions architect do to implement least privilege access?

- A. Update the permission policy on the SQS queue to give write access to the vendor's AWS account.
- B. Create an IAM user with write access to the SQS queue and share the credentials for the IAM user.
- C. Update AWS Resource Access Manager to provide write access to the SQS queue from the vendor's AWS account.
- D. Create a cross-account role with access to all SQS queues and use the vendor's AWS account in the trust document for the role.

A

Question #339

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.

The tracking will need to read as fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of packages might be tracked on other days. Tracking will need to be searchable by tracking ID, customer ID, and order ID. Order older than 1 month no longer need to be tracked.

What should a solution architect recommend to accomplish this with minimal cost of ownership?

- A. Use Amazon DynamoDB Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
- B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.
- C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
- D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

B

Question #340

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

C

Question #341

A company needs to store data in Amazon S3. A compliance requirement states that when any changes are made to objects the previous state of the object with any changes must be preserved. Additionally, files older than 5 years should not be accessed but need to be archived for auditing. What should a solutions architect recommend that is MOST cost-effective?

- A. Enable object-level versioning and S3 Object Lock in governance mode
- B. Enable object-level versioning and S3 Object Lock in compliance mode
- C. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive
- D. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

C

Question #342

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

DE

Question #343

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not

be used on most mornings in the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur they will happen very quickly.

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

A

Question #344

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

C

Question #345

A company is preparing to deploy a new serverless workload. A solutions architect needs to configure permissions for invoking an AWS Lambda function. The function will be triggered by an Amazon EventBridge (Amazon CloudWatch Events) rule. Permissions should be configured using the principle of least privilege.

Which solution will meet these requirements?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:eventsamazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda: as the action and Service:events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

D

Question #346

A company is building its web application using containers on AWS. The company requires three instances of the web application to run at all times. The application must be able to scale to meet increases in demand. Management is extremely sensitive to cost but agrees that the application should be highly available.

What should a solutions architect recommend?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

A

Question #347

A company is Re-architecting a strongly coupled application to be loosely coupled. Previously the application used a request/response pattern to communicate between tiers. The company plans to use Amazon Simple Queue Service (Amazon SQS) to achieve decoupling requirements. The initial design contains one queue for requests and one for responses. However, this approach is not processing all the messages as the application scales.

What should a solutions architect do to resolve this issue?

- A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.
- B. Configure a FIFO queue, and use the message deduplication ID and message group ID.
- C. Create a temporary queue, with the Temporary Queue Client to receive each response message.
- D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

C

Question #348

A company is launching an ecommerce website on AWS. This website is built with a three-tier architecture that includes a MySQL database in a Multi-AZ deployment of Amazon Aurora MySQL. The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones. The application produces a metric that describes the load the application experiences.

Which solution meets these requirements?

- A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling
- B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
- C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.
- D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

D

Question #349

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

C

Question #350

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B.

B.

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

- A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

B

Question #351

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3. Which solution meets these requirements and is MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

B

Question #352

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

Which solution meets these requirements?

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

A

Question #353

A company has multiple applications that use Amazon RDS for MySQL as its database. The company recently discovered that a new custom reporting application has increased the number of Queries on the database. This is slowing down performance.

How should a solutions architect resolve this issue with the LEAST amount of application changes?

- A. Add a secondary DB instance using Multi-AZ.
- B. Set up a read replica and Multi-AZ on Amazon RDS.
- C. Set up a standby replica and Multi-AZ on Amazon RDS.
- D. Use caching on Amazon RDS to improve the overall performance.

B

Question #354

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that security and compliance standards are being followed throughout the development process.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.
- B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.
- C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

C

Question #355

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month.

Which analytics strategy is MOST cost-effective for the company to use?

- A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.
- B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.
- C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.

D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

Question #356

B

A company wants to move its on-premises network, attached storage (NAS) to AWS. The company wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time.

Which solution meets these requirements and is MOST cost-effective?

- A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.
- B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.
- C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.
- D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

D

Question #357

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.

How should the company write its application to handle these database requests?

- A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
- B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

D

Question #358

A company that recently started using AWS establishes a Site-to-Site VPN between its on-premises datacenter and AWS. The company's security mandate states that traffic originating from on premises should stay within the company's private IP space when communicating with an Amazon Elastic Container Service (Amazon ECS) cluster that is hosting a sample web application.

Which solution meets this requirement?

- A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.
- B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.
- C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by

using VPC peering.

D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

B

Question #359

A solutions architect must analyze and update a company's existing IAM policies prior to deploying a new workload. The solutions architect created the following policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Deny",  
    "NotAction": "s3:PutObject",  
    "Resource": "*",  
    "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}  
  }]  
}
```

What is the net effect of this policy?

- A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.
- C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

D

Question #360

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a

PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

AE

Question #361

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

D

Question #362

A company is using Amazon DynamoDB with provisioned throughput for the database tier of its ecommerce website. During flash sales, customers experience periods of time when the database cannot handle the high number of transactions taking place. This causes the company to lose transactions. During normal periods, the database performs appropriately.

Which solution solves the performance problem the company faces?

- A. Switch DynamoDB to on-demand mode during flash sales.
- B. Implement DynamoDB Accelerator for fast in memory performance.
- C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.
- D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

A

Question #363

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

B

Question #364

A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.

What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

- A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
- B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access

(S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

B

Question #365

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue

Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

- A. Create an instance profile that provides the other company access to the SQS queue.
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

C

Question #366

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and a paid tier.

Users in the paid tier will have their videos converted first and then the free tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

- A. One FIFO queue for the paid tier and one standard queue for the free tier.
- B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

D

Question #367

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts.

Which AWS service can the administrator use to protect the company against attacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

B

Question #368

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances. What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table.
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

D

Question #369

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon

Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

C

Question #370

A company wants to host its web application on AWS using multiple Amazon EC2 instances across different AWS Regions. Since the application content will be specific to each geographic region, the client requests need to be routed to the server that hosts the content for that clients Region.

What should a solutions architect do to accomplish this?

- A. Configure Amazon Route 53 with a latency routing policy.
- B. Configure Amazon Route 53 with a weighted routing policy.
- C. Configure Amazon Route 53 with a geolocation routing policy.
- D. Configure Amazon Route 53 with a multivalue answer routing policy

C

Question #371

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability.

Which solution meets these requirements?

- A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
- B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
- C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
- D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

A

Question #372

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs. What should a solutions architect recommend to accomplish this?

- A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
- B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
- C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.
- D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

C

Question #373

A company is building a payment application that must be highly available even during regional service disruptions. A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions. The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports. The development team also needs to use SQL.

Which data storage solution meets these requirements?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon S3 with cross-Region replication and Amazon Athena
- D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

A

Question #374

A company stores call recordings on a monthly basis. Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year.

Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost.

Which solution is MOST cost-effective?

- A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier Query S3 Glacier tags and retrieve the files from S3 Glacier.
- B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
- C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

B

Question #375

A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

- A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.
- B. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events. AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.
- C. The requests from the API are sent to the models' Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.
- D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue. AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

D

Question #376

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

- A. Amazon S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

D

Question #377

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an

Elastic Load Balancer (ELB). A third party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

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

D

Question #378

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance.

Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

C

Question #379

A company is running a multi-tier web application on AWS. The application runs its database tier on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region. A database administrator who regularly monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica and causing increased read latency of the application.

What should a solutions architect do to improve read scalability?

- A. Reboot the Aurora DB cluster.
- B. Create a cross-Region read replica.
- C. Increase the instance class of the read replica.
- D. Configure Aurora Auto Scaling for the read replica.

D

Question #380

A company's order fulfillment service uses a MySQL database. The database needs to support a large number of concurrent queries and transactions. Developers are spending time patching and tuning the database. This is causing delays in releasing new product features.

The company wants to use cloud-based services to help address this new challenge. The solution must allow the developers to migrate the database with little or no code changes and must optimize performance.

Which service should a solutions architect use to meet these requirements?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon ElastiCache
- D. MySQL on Amazon EC2

A

Question #381

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company want to run complex transformation before transferring the data.

Which AWS service should a solutions architect recommend for this migration?

- A. AWS Snowball
- B. AWS Snowmobile
- C. AWS Snowball Edge Storage Optimize
- D. AWS Snowball Edge Compute Optimize

D

Question #382

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

A

Question #383

A company is selling up an application to use an Amazon RDS MySQL DB instance. The database must be architected for high availability across Availability Zones and AWS Regions with minimal downtime.

How should a solutions architect meet this requirement?

- A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.
- B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.
- C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.
- D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

B

Question #384

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multi-value routing policy
- D. Geolocation routing policy

C

Question #385

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

What should a solutions architect do to migrate and store the data at the LOWEST cost?

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

A

Question #386

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states:

- Keys must be rotated every 90 days.
- Strict separation of duties between key users and key administrators must be implemented.
- Auditing key usage must be possible.

What should the solutions architect recommend?

- A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
- C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
- D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

A

Question #387

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

Which storage solution is MOST cost-effective?

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

C

Question #388

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in

the same Region.

D

Question #389

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in older. What should a solutions architect recommend to decouple the system?

- A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.
- B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.
- D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

C

Question #390

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy.

Which solution meets these requirements?

- A. Replace the NAT gateway with a NAT instance.
- B. Replace the NAT gateway with an internet gateway.
- C. Replace the NAT gateway with a gateway VPC endpoint.
- D. Replace the NAT gateway with an AWS Direct Connect connection.

C

Question #391

A company hosts a website on premises and wants to migrate it to the AWS Cloud. The website exposes a single hostname to the internet but it routes its functions to different on-premises server groups based on the path of the URL. The server groups are scaled independently depending on the needs of the functions they support. The company has an AWS Direct Connect connection configured to its on-premises network.

What should a solutions architect do to provide path-based routing to send the traffic to the correct group of servers?

- A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.
- B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.
- C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.
- D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer

for the group of servers supporting that path.

C

Question #392

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage auto scaling in RDS.
- B. Increase the RDS database instance size.
- C. Change the RDS database instance storage type to Provisioned IOPS.
- D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

A

Question #393

An ecommerce website is deploying its web application as Amazon Elastic Container Service (Amazon ECS) container instances behind an Application Load Balancer (ALB). During periods of high activity, the website slows down and availability is reduced. A solutions architect uses Amazon CloudWatch alarms to receive notifications whenever there is an availability issue so they can scale out resources. Company management wants a solution that automatically responds to such events.
Which solution meets these requirements?

- A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

C

Question #394

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results. A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the

database read endpoints.

- C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.
- D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on-demand capacity scaling enabled.

A

Question #395

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions. What should a solutions architect recommend to improve application resiliency?

- A. Modify the shipping application to write to a local database.
- B. Modify the application APIs to run serverless using AWS Lambda
- C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
- D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

D

Question #396

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to

Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB.
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

A

Question #397

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every

transaction and then store the transactions data in AmazonDynamoDB. Other applications can consume the transactions data off the Kinesis data stream.

D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

C

Question #398

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
- B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
- C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
- D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

D

Question #399

A web application must persist order data to Amazon S3 to support near-real time processing. A solutions architect needs to create an architecture that is both scalable and fault tolerant.

Which solutions meet these requirements? (Choose two.)

- A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

CE

Question #400

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions. To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.

What should a solutions architect do to accomplish this?

- A. Create a NAT gateway and update the route table of the EC2 instances' subnet.
- B. Create a VPC endpoint and update the route table of the EC2 instances' subnet.
- C. Create a VPN connection and update the route table of the EC2 instances' subnet.
- D. Create a VPC peering connection and update the route table of the EC2 instances' subnet.

B

Question #401

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.

Which application change should a solutions architect recommend to resolve these issues?

- A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
- B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
- C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
- D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

C

Question #402

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

D

Question #403

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's .NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

- A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.
- B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
- C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

B

Question #404

A company has an application running on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3. To reduce costs, the company wants to configure its AWS resources in a cost-effective manner.

How should the company accomplish this?

- A. Deploy a NAT gateway to access the S3 buckets.
- B. Deploy AWS Storage Gateway to access the S3 buckets.
- C. Deploy an S3 gateway endpoint to access the S3 buckets.
- D. Deploy an S3 interface endpoint to access the S3 buckets.

C

Question #405

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment.

What should a solutions architect recommend?

- A. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
- B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
- D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

B

Question #406

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solutions architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

- A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
- B. Build the application to use Amazon Lightsail with On-Demand Instances.
- C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.
- D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

D

Question #407

A company is using Site-to-Site VPN connections for secure connectivity to its AWS Cloud resources from on premises. Due to an increase in traffic across the VPN connections to the Amazon EC2 instances, users are experiencing slower VPN connectivity. Which solution will improve the VPN throughput?

- A. Implement multiple customer gateways for the same network to scale the throughput.
- B. Use a transit gateway with equal cost multipath routing and add additional VPN tunnels.
- C. Configure a virtual private gateway with equal cost multipath routing and multiple channels.
- D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

B

Question #408

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots replication and sub-millisecond response times. What should the solutions architect recommend to solve these issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

C

Question #409

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.
- B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC

endpoint.

D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

C

Question #410

A company is deploying an application in three AWS Regions using an Application Load Balancer Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy.
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

A

Question #411

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS

Key Management Service Customer Master Keys (AWS KMS CMKs). A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy.
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

BE

Question #412

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. To meet the migration date, minimal changes can be made.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web server.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
- D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

C

Question #413

A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the internet, and a VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch.

Which solution meets these requirements?

- A. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to each target group of each ALB. Route with Amazon Route 53 based on the URL query string.
- B. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to the target group of each ALB. Create a software router on an EC2 instance based on the URL query string.
- C. Use one ALB with two target groups: one for the AWS resource and one for on-premises. Add hosts to each target group of the ALB. Configure listener rules based on the URL query string.
- D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on-premises. Add hosts to each Auto Scaling group. Route with Amazon Route 53 based on the URL query string.

C

Question #414

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.

Which solution meets these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
- B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
- C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

C

Question #415

A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

- A. Use AWS Snowball Edge devices to process and store the images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2

instances for processing the images.

D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

A

Question #416

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application, data layer that uses Oracle-specific PSQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

AD

Question #417

An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.

How should the permissions for the team be configured so they also adhere to the concept of least privilege?

- A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.
- B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group.
- C. Create an execution role for the Lambda functions. Attach a managed policy that has permission boundaries specific to these Lambda functions.
- D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions. Allow the engineering team to assume this role.

D

Question #418

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains over 10 million rows. The database has 2 TB of General Purpose SSD (gp2) storage. There are millions of updates against this data every day through the company's website. The company has noticed some operations are taking 10 seconds or longer and has determined that the database storage performance is the bottleneck.

Which solution addresses the performance issue?

- A. Change the storage type to Provisioned IOPS SSD (io1).
- B. Change the instance to a memory-optimized instance class.

- C. Change the instance to a burstable performance DB instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

A

Question #419

A company has an Amazon S3 bucket that contains mission-critical data. The company wants to ensure this data is protected from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

AB

Question #420

A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.

The application development team does not have time to make the necessary code modifications to move the application to AWS.

Which service should a solutions architect recommend to allow the application to copy files to AWS?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Windows File Server
- C. AWS Snowball
- D. AWS Storage Gateway

D

Question #421

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- B. Create a bucket policy to make the objects in the S3 bucket public.
- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

AC

Question #422

A solutions architect plans to convert a company's monolithic web application into a multi-tier application. The company wants to avoid managing its own infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application's API.

Which solution meets these requirements?

- A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
- B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
- C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
- D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

B

Question #423

A team has an application that detects new objects being uploaded into an Amazon S3 bucket. The uploads trigger AWS Lambda function to write object metadata into an Amazon DynamoDB table and an Amazon RDS for PostgreSQL database.

Which action should the team take to ensure high availability?

- A. Enable Cross-Region Replication in the S3 bucket.
- B. Create a Lambda function for each Availability Zone the application is deployed in.
- C. Enable Multi-AZ on the RDS for PostgreSQL database.
- D. Create a DynamoDB stream for the DynamoDB table.

C

Question #424

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

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

C

Question #425

An application calls a service run by a vendor. The vendor charges based on the number of calls. The finance department needs to know the number of calls that are made to the service to validate the billing statements.

How can a solutions architect design a system to durably store the number of calls without requiring changes to the application?

- A. Call the service through an internet gateway.
- B. Decouple the application from the service with an Amazon Simple Queue Service (Amazon SQS) queue.
- C. Publish a custom Amazon CloudWatch metric that counts calls to the service.
- D. Call the service through a VPC peering connection.

C

Question #426

A company wants to reduce its Amazon S3 storage costs in its production environment without impacting durability or performance of the stored objects.

What is the FIRST step the company should take to meet these objectives?

- A. Enable Amazon Macie on the business-critical S3 buckets to classify the sensitivity of the objects.
- B. Enable S3 analytics to identify S3 buckets that are candidates for transitioning to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Enable versioning on all business-critical S3 buckets.
- D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

B

Question #427

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

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

D

Question #428

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple

Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of `application` and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

- A. Use AWS CloudTrail to generate a list of resources with the application tag.
- B. Use the AWS CLI to query each service across all Regions to report the tagged components.

- C. Run a query in Amazon CloudWatch Logs Insights to report on the components with the application tag.
- D. Run a query with the AWS Resource Groups Tag Editor to report on the resources globally with the application tag.

D

Question #429

A development team is deploying a new product on AWS and is using AWS Lambda as part of the deployment. The team allocates 512 MB of memory for one of the Lambda functions. With this memory allocation, the function is completed in 2 minutes. The function runs millions of times monthly, and the development team is concerned about cost. The team conducts tests to see how different Lambda memory allocations affect the cost of the function.

Which steps will reduce the Lambda costs for the product? (Choose two.)

- A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.
- B. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 90 seconds.
- C. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 4 minutes.
- D. Increase the memory allocation for this Lambda function to 2,048 MB if this change causes the execution time of each function to be less than 1 minute.
- E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

AC

Question #430

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon

EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

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

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

CD

Question #431

A user owns a MySQL database that is accessed by various clients who expect, at most, 100 ms latency on requests. Once a record is stored in

the database, it is rarely changed. Clients only access one record at a time.

Database access has been increasing exponentially due to increased client demand. The resultant load will soon exceed the capacity of the most expensive hardware available for purchase. The user wants to migrate to AWS, and is willing to change database systems.

Which service would alleviate the database load issue and offer virtually unlimited scalability for the future?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. AWS Data Pipeline

B

Question #432

A company designs a mobile app for its customers to upload photos to a website. The app needs a secure login with multi-factor authentication (MFA). The company wants to limit the initial build time and the maintenance of the solution.

Which solution should a solutions architect recommend to meet these requirements?

- A. Use Amazon Cognito Identity with SMS-based MFA.
- B. Edit IAM policies to require MFA for all users.
- C. Federate IAM against the corporate Active Directory that requires MFA.
- D. Use Amazon API Gateway and require server-side encryption (SSE) for photos.

A

Question #433

A company has an application that uses overnight digital images of products on store shelves to analyze inventory data. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) and obtains the images from an Amazon S3 bucket for its metadata to be processed by worker nodes for analysis. A solutions architect needs to ensure that every image is processed by the worker nodes.

What should the solutions architect do to meet this requirement in the MOST cost-efficient way?

- A. Send the image metadata from the application directly to a second ALB for the worker nodes that use an Auto Scaling group of EC2 Spot Instances as the target group.
- B. Process the image metadata by sending it directly to EC2 Reserved Instances in an Auto Scaling group. With a dynamic scaling policy, use an Amazon CloudWatch metric for average CPU utilization of the Auto Scaling group as soon as the front-end application obtains the images.
- C. Write messages to Amazon Simple Queue Service (Amazon SQS) when the front-end application obtains an image. Process the images with EC2 On-Demand instances in an Auto Scaling group with instance scale-in protection and a fixed number of instances with periodic health checks.
- D. Write messages to Amazon Simple Queue Service (Amazon SQS) when the application obtains an image. Process the images with EC2 Spot Instances in an Auto Scaling group with instance scale-in protection and a dynamic scaling policy using a custom Amazon CloudWatch metric for the current number of messages in the queue.

D

Question #434

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of

Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing.

Which solution will meet these requirements?

- A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
- B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
- C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
- D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

C

Question #435

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

A

Question #436

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations. Which solution meets these requirements?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

A

Question #437

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure.

Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

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

A

Question #438

A company has two AWS accounts: Production and Development. There are code changes ready in the Development account to push to the Production account.

In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers might need access to perform testing as well.

What should a solutions architect recommend?

- A. Create two policy documents using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Give one IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account with the trust policy that specifies the Development account. Allow developers to assume the role.
- D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account. Add developers to the group.

C

Question #439

A company is using an Amazon S3 bucket to store data uploaded by different departments from multiple locations. During an AWS Well-Architected review, the financial manager notices that 10 TB of S3 Standard storage data has been charged each month. However, in the AWS Management Console for Amazon S3, using the command to select all files and folders shows a total size of 5 TB.

What are the possible causes for this difference? (Choose two.)

- A. Some files are stored with deduplication.
- B. The S3 bucket has versioning enabled.
- C. There are incomplete S3 multipart uploads.
- D. The S3 bucket has AWS Key Management Service (AWS KMS) enabled.
- E. The S3 bucket has Intelligent-Tiering enabled.

BC

Question #440

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.

Which solution meets these requirements?

- A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
- D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

A

Question #441

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
- B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
- C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
- D. Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

C

Question #442

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these

VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC

communication.

- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

C

Question #443

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.

Which combination of network solutions will meet these requirements? (Choose two.)

- A. Enable and configure enhanced networking on each EC2 instance.
- B. Group the EC2 instances in separate accounts.
- C. Run the EC2 instances in a cluster placement group.
- D. Attach multiple elastic network interfaces to each EC2 instance.
- E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

AC

Question #444

A company is running a global application. The application's users submit multiple videos that are then merged into a single video file. The application uses a single Amazon S3 bucket in the us-east-1 Region to receive uploads from users. The same S3 bucket provides the download location of the single video file that is produced. The final video file output has an average size of 250 GB.

The company needs to develop a solution that delivers faster uploads and downloads of the video files that are stored in Amazon S3. The company will offer the solution as a subscription to users who want to pay for the increased speed.

What should a solutions architect do to meet these requirements?

- A. Enable AWS Global Accelerator for the S3 endpoint. Adjust the application's upload and download links to use the Global Accelerator S3 endpoint for users who have a subscription.
- B. Enable S3 Cross-Region Replication to S3 buckets in all other AWS Regions. Use an Amazon Route 53 geolocation routing policy to route S3 requests based on the location of users who have a subscription.
- C. Create an Amazon CloudFront distribution and use the S3 bucket in us-east-1 as an origin. Adjust the application to use the CloudFront URL as the upload and download links for users who have a subscription.
- D. Enable S3 Transfer Acceleration for the S3 bucket in us-east-1. Configure the application to use the bucket's S3-accelerate endpoint domain name for the upload and download links for users who have a subscription.

D

Question #445

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Sid": "2",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}

```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

D

Question #446

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

C

Question #447

A company is using AWS Organizations with two AWS accounts: Logistics and Sales. The Logistics account operates an Amazon Redshift cluster. The Sales account includes Amazon EC2 instances. The Sales account needs to access the Logistics account's Amazon Redshift cluster.

What should a solutions architect recommend to meet this requirement MOST cost-effectively?

- A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data.
- B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account.
- C. Create a snapshot of the Amazon Redshift cluster, and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account.
- D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account.

A

Question #448

A company is using Amazon Redshift for analytics and to generate customer reports. The company recently acquired 50 TB of additional customer demographic data. The data is stored in .csv files in Amazon S3. The company needs a solution that joins the data and visualizes the results with the least possible cost and effort.

What should a solutions architect recommend to meet these requirements?

- A. Use Amazon Redshift Spectrum to query the data in Amazon S3 directly and join that data with the existing data in Amazon Redshift. Use Amazon QuickSight to build the visualizations.
- B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSight to join the data from Athena with the existing data in Amazon Redshift and to build the visualizations.
- C. Increase the size of the Amazon Redshift cluster, and load the data from Amazon S3. Use Amazon EMR Notebooks to query the data and build the visualizations in Amazon Redshift.
- D. Export the data from the Amazon Redshift cluster into Apache Parquet files in Amazon S3. Use Amazon Elasticsearch Service (Amazon ES) to query the data. Use Kibana to visualize the results.

A

Question #449

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners.

Which solution meets these requirements?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.
- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

A

Question #450

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to fail over to us-west-2 with a recovery time objective (RTO) of 15 minutes.

What should a solutions architect recommend to meet these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and use-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

D

Question #451

A company is migrating its applications to AWS. Currently, applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system. The company is running an analytics application in the cloud that runs hourly to generate insights from this data. The company needs a solution to handle the ongoing data transfer between the on-premises shared file system and Amazon S3. The solution also must be able to handle occasional interruptions in internet connectivity.

Which solutions should the company use for the data transfer to meet these requirements?

- A. AWS DataSync
- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

A

Question #452

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database. What should the solutions architect do to ensure that the website can scale with increasing traffic? (Choose two.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

BE

Question #453

A company captures ordered clickstream data from multiple websites and uses batch processing to analyze the data. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data.

The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.

Which combination of AWS services will meet these requirements MOST cost-effectively? (Choose two.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

DE

Question #454

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company's IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.

What should a solutions architect do to secure the data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

B

Question #455

A company with a single AWS account runs its internet-facing containerized web application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

The EKS cluster is placed in a private subnet of a VPC. System administrators access the EKS cluster through a bastion host on a public subnet. A new corporate security policy requires the company to avoid the use of bastion hosts. The company also must not allow internet connectivity to the EKS cluster.

Which solution meets these requirements MOST cost-effectively?

- A. Set up an AWS Direct Connect connection.
- B. Create a transit gateway.
- C. Establish a VPN connection.
- D. Use AWS Storage Gateway.

C

Question #456

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

D

Question #457

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process. The company's network team has ruled out bandwidth as a limiting factor.

Which actions should the solutions architect take to speed up the migration? (Choose two.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

AC



We help to get you certified in IT Technologies AWS, Azure, GCP, Oracle and Many more exams

SAA-C02

AWS Certified Solutions Architect - Associate

1. A Company has an AWS Direct Connect connection from its corporate data center to its VPC in the us-east-1 Region. The company recently acquired a corporation that has several VPCs and a Direct connect Connection between its on-premises data center and the eu-west-2 Region. The CIDR blocks for the VPCs of the company and the corporation do not overlap. The company requires connectivity between two Regions and the data centers. The company needs a solution that is scalable while reducing operational overhead.

What should a solutions architect do to meet these requirements?

- A. Set up inter-Region VPC peering between the VPC in us-east-1 and the VPCs in eu-west-2.
- B. Create private virtual interfaces from the Direct Connect connection in us-east-1 to the VPCs in eu-west-2.

C. Establish VPN appliances in a fully meshed VPN network hosted by Amazon EC2. Use AWS VPN CloudHub to send and receive data between the data centers and each VPC.

D. Connect the existing Direct connect connection to a Direct Connect gateway. Route traffic from the virtual private gateways of the VPCs in each Region to the Direct Connect gateway.

Ans: C

2. A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.

A development team recently created a AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

A. Configure the Lambda function to run in the VPC with the appropriate security group.

B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.

C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect

D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Ans : D

3. A company needs to build a reporting solution on AWS. The solution must support SQL queries that data analysts run on the data. The data analysts will run fewer than 10 total queries each day. The company generates 3 GB of new data daily in an on-premises relational database. This data needs to be transferred to the AWS to perform reporting tasks.

What should a solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database into Amazon S3. Use Amazon Athena to query the data.
- B. Use an Amazon Kinesis data Firehose delivery stream to deliver the data into an Amazon Elasticsearch Service (Amazon ES) cluster. Run the queries in Amazon ES.
- C. Export a daily copy of the data from the on-premises database. Use an AWS storage Gateway file gateway to store and copy the export into Amazon S3. Use an Amazon EMR cluster to query the data.
- D. Use AWS Database Migration Service (AWS DMS) to replicate the data from the on-premises database and load it into an Amazon Redshift cluster. Use the Amazon Redshift cluster to query the data.

Ans : A

4. A company finds that, as its use of Amazon EC2 instances grows, its Amazon Elastic Block Store (Amazon EBS) storage costs increasing faster than expected.

Which EBS management practices would help reduce costs? (Select TWO)

- A. Convert the EBS volumes to an EC2 instance store.
- B. Monitor and enforce that the `DeletionOnTermination` attribute is set to true for all EBS volumes, unless persistence requirements dictate otherwise.
- C. Purchase an EC2 Instance Saving Plan for all EBS volumes that are serving persistent business requirements.
- D. For EBS volumes needed for retention purposes that are not being actively used, take a snapshot and terminate the instance and volume.
- E. Convert the existing EBS volumes to EBS Provisioned IOPS SSD (io1).

Ans : BD

5. A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

- A. Use standard SQL queries in Amazon Athena to analyze the CloudFront Logs in the S3 bucket. Visualize the results with AWS Glue.
- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 Bucket. Visualize the results with Amazon QuickSight.
- C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS QuickSight.

Ans : A

6. A company is planning to make a series of schema changes to tables on its Amazon Aurora DB cluster. A solutions architect needs to test the changes in the most cost-effective manner possible.

What should the solutions architect do to meet these requirements?

- A. Create a clone of the current Aurora DB cluster. Perform the schema changes on the clone. Once the changes are tested and performance is acceptable, apply the same changes on the original cluster. Delete the clone.
- B. Create an Amazon RDS for MySQL replica. Perform the schema changes on the replica. Once the changes are tested and performance is acceptable, apply the same changes on the primary DB instance. Delete the replica.
- C. Create an additional Aurora Replica. Perform the schema changes on the Aurora Replica. Once the changes are tested and performance is acceptable apply the same changes on the primary DB instance. Delete the Aurora Replica.
- D. Take a snapshot of the current Aurora DB cluster. Restore the snapshot of the cluster to a new cluster. Perform the schema changes on the restored cluster. Once the changes are tested and performance is acceptable, apply the same changes on the original cluster. Delete the resorted cluster.

Ans : C

7. A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.

Which combination of network solutions will meet these requirements? (Select TWO)

- A. Distribute the EC2 instances across multiple Availability Zones.
- B. Attach an Elastic Fabric Adapter (EFA) to each EC2 instance.
- C. Place the EC2 instances in a single Availability Zone.
- E. Run the EC2 instances in a cluster placement group.

Ans : CD

8. A company wants to run a static website served through Amazon CloudFront.

What is an advantage of storing the website content in an Amazon S3 bucket instead of an Amazon Elastic Block Store (Amazon EBS) volume?

- A. S3 buckets are replicated globally, allowing for large scalability. EBS volumes are replicated only within an AWS Region.
- B. S3 is an origin for cloudFront. EBS volumes would need EC2 instance behind an Elastic Load Balancing load balancer to be an origin.
- C. S3 buckets can be encrypted, allowing for secure storage of the web files. EBS volumes cannot be encrypted.
- D. S3 buckets support object-level read throttling, preventing abuse. EBS volumes do not provide object-level throttling.

Answer : A

9. A company's cloud operations team wants to standardize resource remediation. The company wants to provide a standard governance evaluations and remediation's to all member accounts in its organization in AWS organizations.

Which self-managed AWS service can be company use to meet these requirements with the LEAST amount of operations.

- A. AWS Security Hub compliance standards
- B. AWS Config conformance packs
- C. AWS CloudTrail
- D. AWS Trusted Advisor

Answer : D

10. A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone and configure AWS Data migration Service (AWS DMS) change data capture (CDC) tasks.

Answer : A

11. A company has concerns about its Amazon RDS database. The workload is unpredictable, and periodic floods of new can cause the company to run out of storage. The database runs on a general purpose instance with 300 GiB of storage.

What should a solutions architect recommend to the company?

- A. Enable RDS storage autoscaling.
- B. Schedule vertical instance scaling.
- C. Change to a storage optimized instance type and vertically scale the database.

D. Configure an AWS Lambda function to increase RDS storage by 1 GB when storage space is low.

Answer : A

12. A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application in multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.

The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain single primary reservation database that is globally consistent.

Which solution should a solutions architect recommend to meet these requirements?

A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment.

B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

C. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.

D. Migrate the application to an Amazon aurora serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use Aws Lambda functions to process event streams in each Region to synchronize the databases.

Answer : A

13. A solutions architect is designing an architecture that includes web, application, and database tiers. The web tier must be an auto scaling. The solutions architect has decided to separate each tier into its own subnets. The design includes two public and four private subnets.

The security team requires that tiers be able to communicate with each other only when there is a business need and that all to the network traffic be blocked.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon GuardDuty source/destination rule set to control communication.
- B. Create one security group for all tiers to limit traffic to only the required source destinations.
- C. Create specific security groups for each tier to limit traffic to only the required source and destinations.
- D. Create network ACLs in all six subnets to limit traffic to the sources and destinations required for the application to function.

Answer : D

14. A company's security policy requires that all AWS API activity in its AWS accounts be recorded for periodic auditing. Which needs to ensure that AWS CloudTrail is enabled on all of its current and future AWS accounts using AWS Organization.

Which solution is MOST secure?

- A. At the organization's root, define and attach a service control policy (SCP) that permits enabling CloudTrail on
- B. Create IAM groups in the organization's master account as needed. Define and attach an IAM policy to the group to prevent users from disabling CloudTrail.
- C. Organize accounts into organizational units (OUs). At the organization's root, define and attach a service control policy (SCP) that prevents users from disabling CloudTrail.
- D. Add all existing accounts under the organization's root. Define and attach a service control policy (SCP) to every that prevents users from disabling CloudTrail.

Answer : B

Question #1

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's

DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Answer: *B*

Active-passive failover -

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route 53 responds to DNS queries using the secondary record.

How Amazon Route 53 averts cascading failures

As a first defense against cascading failures, each request routing algorithm (such as weighted and failover) has a mode of last resort. In this special mode, when all records are considered unhealthy, the Route 53 algorithm reverts to considering all records healthy.

For example, if all instances of an application, on several hosts, are rejecting health check requests, Route 53 DNS servers will choose an answer anyway and return it rather than returning no DNS answer or returning an NXDOMAIN (non-existent domain) response. An application can respond to users but still fail health checks, so this provides some protection against misconfiguration.

Similarly, if an application is overloaded, and one out of three endpoints fails its health checks, so that it's excluded from Route 53 DNS responses, Route 53 distributes responses between the two remaining endpoints. If the remaining endpoints are unable to handle the additional load and they fail, Route 53 reverts to distributing requests to all three endpoints.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-problems.html>

Additional New

A company runs an internet-facing web application on AWS. The company uses Amazon Route 53 for DNS management and has a public hosted zone to route traffic from the internet to the application. The company wants to log DNS response codes to help system administrators perform any root cause analysis in the future.

Which solution will meet these requirements?

- A. Use Route 53 to configure query logging.
- B. Use AWS CloudTrail to record all Route 53 queries.
- C. Use Amazon CloudWatch to collect and process Route 53 metrics.
- D. Use AWS Trusted Advisor to perform on-demand root cause analysis.

2

A developer is creating an AWS Lambda function to perform dynamic updates to a database when an item is added to an Amazon Simple Queue Service (Amazon SQS) queue. A solutions architect must recommend a solution that tracks any usage of database credentials in AWS CloudTrail. The solution also must provide auditing capabilities.

Which solution will meet these requirements?

- A. Store the encrypted credentials in a Lambda environment variable.
- B. Create an Amazon DynamoDB table to store the credentials. Encrypt the table.
- C. Store the credentials as a secure string in AWS Systems Manager Parameter Store.
- D. Use an AWS Key Management Service (AWS KMS) key store to store the credentials.

3.

A company has an AWS Direct Connect connection from its on-premises location to an AWS account. The AWS account has 30 different VPCs in the same AWS Region. The VPCs use private virtual interfaces (VIFs). Each VPC has a CIDR block that does not overlap with other networks under the company's control.

The company wants to centrally manage the networking architecture while still allowing each VPC to communicate with all other VPCs and on-premises networks.

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

-
- A. Create a transit gateway, and associate the Direct Connect connection with a new transit VIF. Turn on the transit gateway's route propagation feature.
 - B. Create a Direct Connect gateway. Recreate the private VIFs to use the new gateway. Associate each VPC by creating new virtual private gateways.
 - C. Create a transit VPC. Connect the Direct Connect connection to the transit VPC. Create a peering connection between all other VPCs in the Region. Update the route tables.
 - D. Create AWS Site-to-Site VPN connectless from on-premises to each VPC. Ensure that both VPN tunnels are UP for each connection. Turn on the route propagation feature.

4.

A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meets these requirements?

- Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
- Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
- Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
- Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

5.

A company wants to use a custom distributed application that calculates various profit and loss scenarios. To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances. The connection must minimize latency and must maximize throughput.

Which solution will meet these requirements?

- Provision the application to use EC2 Dedicated Hosts of the same instance type.
- Configure a placement group for EC2 instances that have the same instance type.
- Use multiple AWS elastic network interfaces and link aggregation.
- Configure AWS PrivateLink for the EC2 instances.

6.

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Select TWO.)

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

Question #2

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Answer: A

Placement groups -

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Depending on the type of workload.

Cluster " packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Question #3

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world.

Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance. What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Answer: C

Reference:

<https://aws.amazon.com/ec2/autoscaling/>

Question #4

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Answer: B

Migrating Existing Files to Amazon FSx for Windows File Server Using AWS DataSync

We recommend using AWS DataSync to transfer data between Amazon FSx for Windows File Server file systems. DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and other AWS storage services over the internet or AWS Direct Connect. DataSync can transfer your file system data and metadata, such as ownership, time stamps, and access permissions.

Reference:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

Question #5

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Answer: D

Question #6

A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services are MOST cost-effective for this solution? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Answer: DE

Kinesis Data Streams and Kinesis Client Library (KCL) – Data from the data source can be continuously captured and streamed in near real-time using Kinesis Data Streams. With the Kinesis Client Library (KCL), you can build your own application that can preprocess the streaming data as they arrive and emit the data for generating incremental views and downstream analysis.

Kinesis Data Analytics – This service provides the easiest way to process the data that is streaming through Kinesis Data Stream or Kinesis Data Firehose using SQL. This enables customers to gain actionable insight in near real-time from the incremental stream before storing it in Amazon S3.

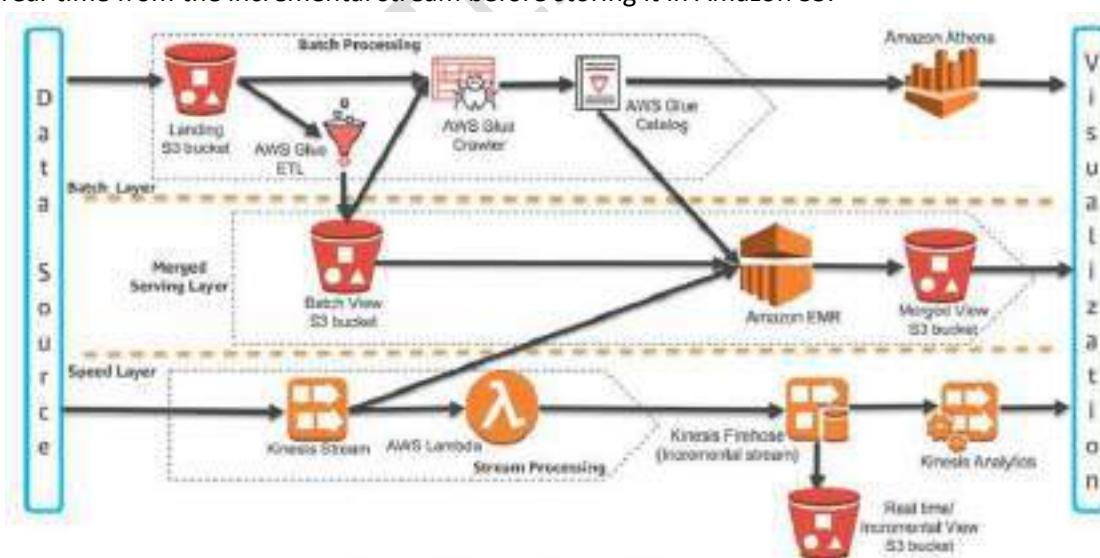


Figure 2: Lambda Architecture Building Blocks on AWS

Reference:

<https://d1.awsstatic.com/whitepapers/lambdacore-on-for-batch-aws.pdf>

Question #7

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Answer: C

Scheduled Scaling for Amazon EC2 Auto Scaling

Scheduled scaling allows you to set your own scaling schedule. For example, let's say that every week the traffic to your web application starts to increase on

Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Question #8

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Choose two.)

- A. Add AWS Shield.
- B. Add Aurora Replica.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Answer: BE

AWS Global Accelerator -

Acceleration for latency-sensitive applications

Many applications, especially in areas such as gaming, media, mobile apps, and financials, require very low latency for a great user experience. To improve the user experience, Global Accelerator directs user traffic to the application endpoint that is nearest to the client, which reduces internet latency and jitter. Global Accelerator routes traffic to the closest edge location by using Anycast, and then routes it to the closest regional endpoint over the AWS global network. Global

Accelerator quickly reacts to changes in network performance to improve your users' application performance.

Amazon CloudFront -

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

Question #9

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Answer: C

Amazon RDS Read Replicas -

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as

Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source

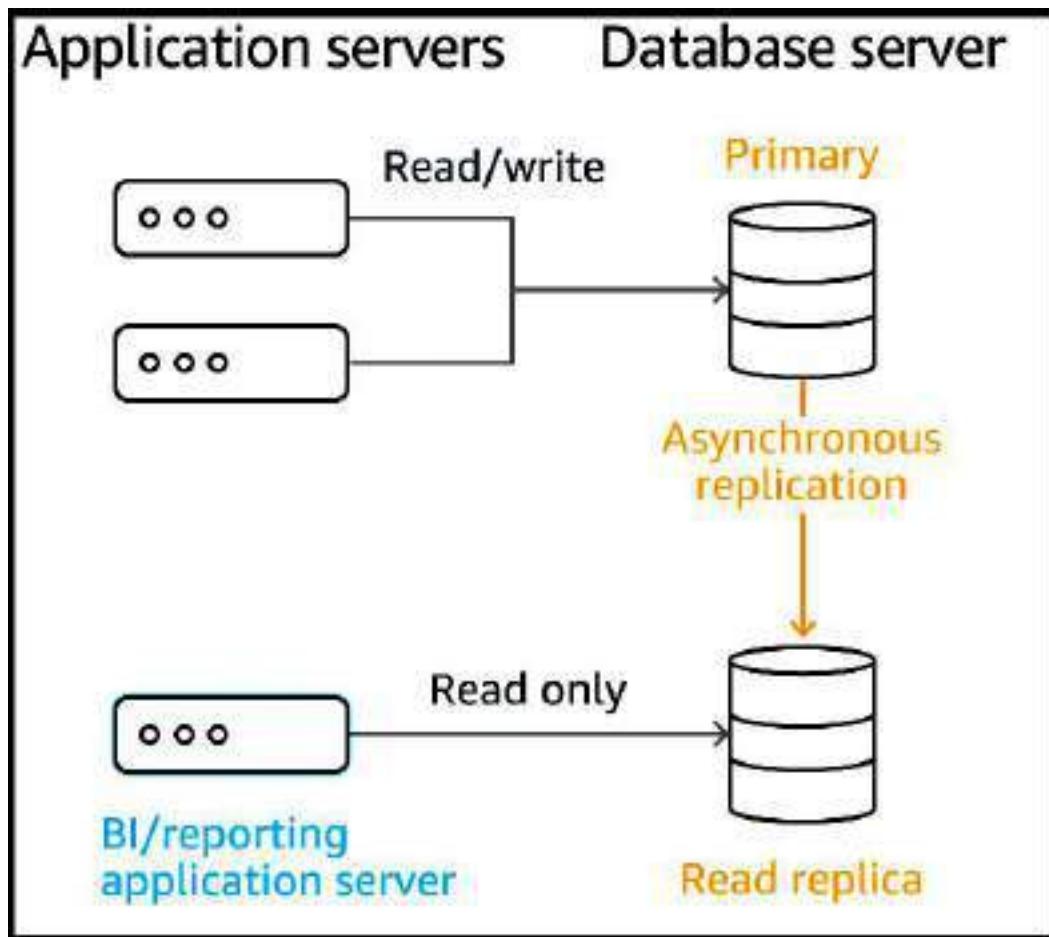
DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-

only connections; applications can connect to a read replica just as they would to any DB instance.

Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon

Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the online documentation.



Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

<https://aws.amazon.com/rds/features/read-relicas/>

Question #10

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity.

- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Answer: C

Reference:

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html
<https://aws.amazon.com/directconnect/>

Question #11

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Ok

Answer: C

"block access for certain countries." You can use geo restriction, also known as geo blocking, to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

Question #12

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs?

- A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.

D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

Answer: *B*

Amazon Elastic File System -

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include: big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

Reference:

<https://aws.amazon.com/efs/>

Question #13

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Answer: *C*

Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Starting today, Amazon RDS Read Replicas for MySQL and MariaDB now support Multi-AZ deployments.

Combining Read Replicas with Multi-AZ enables you to build a resilient disaster recovery strategy and simplify

your database engine upgrade process.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

You can also combine Read Replicas with Multi-AZ for your database engine upgrade process. You can create a Read Replica of your production database instance and upgrade it to a new database engine version. When the upgrade is complete, you can stop applications, promote the Read Replica to a standalone database instance, and switch over your applications. Since the database instance is already a Multi-AZ deployment, no additional steps are needed.

Overview of Amazon RDS Read Replicas

Deploying one or more read replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more read replicas.

Serving read traffic while the source DB instance is unavailable. In some cases, your source DB instance might not be able to take I/O requests, for example due to I/O suspension for backups or scheduled maintenance. In these cases, you can direct read traffic to your read replicas. For this use case, keep in mind that the data on the read replica might be "stale" because the source DB instance is unavailable.

Business reporting or data warehousing scenarios where you might want business reporting queries to run against a read replica, rather than your primary, production DB instance.

Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the source DB instance fails.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/> https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #14

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

A. Amazon EBS

B. Amazon EC2 instance store

- C. Amazon EFS
- D. Amazon S3

Answer: *B*

Question #15

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Answer: *D*

Using Amazon S3 Origins, MediaPackage Channels, and Custom Origins for Web Distributions

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price.

You incur regular Amazon S3 charges for storing the objects in the bucket.

Using Amazon S3 Buckets Configured as Website Endpoints for Your Origin

You can set up an Amazon S3 bucket that is configured as a website endpoint as custom origin with CloudFront.

When you configure your CloudFront distribution, for the origin, enter the Amazon S3 static website hosting endpoint for your bucket. This value appears in the

Amazon S3 console, on the Properties tab, in the Static website hosting pane. For example: <http://bucket-name.s3-website-region.amazonaws.com>

For more information about specifying Amazon S3 static website endpoints, see Website endpoints in the Amazon Simple Storage Service Developer Guide.

When you specify the bucket name in this format as your origin, you can use Amazon S3 redirects and Amazon S3 custom error documents. For more information about Amazon S3 features, see the Amazon S3 documentation.

Using an Amazon S3 bucket as your CloudFront origin server doesn't change it in any way. You can still use it as you normally would and you incur regular

Amazon S3 charges.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #16

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Answer: BC

Reference:

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-api-gateway-supports-endpoint-integrations-with-private-vpcs>

Question #17

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Answer: C

Register endpoints for endpoint groups: You register one or more regional resources, such as Application Load Balancers, Network Load Balancers, EC2

Instances, or Elastic IP addresses, in each endpoint group. Then you can set weights to choose how much traffic is routed to each endpoint.

Endpoints in AWS Global Accelerator

Endpoints in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. A static IP address serves as a single point of contact for clients, and Global Accelerator then distributes incoming traffic across healthy endpoints. Global Accelerator directs traffic to endpoints by using the port (or port range) that you specify for the listener that the endpoint group for the endpoint belongs to.

Each endpoint group can have multiple endpoints. You can add each endpoint to multiple endpoint groups, but the endpoint groups must be associated with different listeners.

Global Accelerator continually monitors the health of all endpoints that are included in an endpoint group. It routes traffic only to the active endpoints that are healthy. If Global Accelerator doesn't have any healthy endpoints to route traffic to, it routes traffic to all endpoints.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints.html>

<https://aws.amazon.com/global-accelerator/faqs/>

Question #18

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Answer: B

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS

Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume — there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service — all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging. All you need to do is supply your code in one of the languages that AWS Lambda supports.

Storing your static content with S3 provides a lot of advantages. But to help optimize your application's performance and security while effectively managing cost, we recommend that you also set up Amazon CloudFront to work with your S3 bucket to serve and protect the content. CloudFront is a content delivery network

(CDN) service that delivers static and dynamic web content, video streams, and APIs around the world, securely and at scale. By design, delivering data out of

CloudFront can be more cost effective than delivering it from S3 directly to your users.

CloudFront serves content through a worldwide network of data centers called Edge Locations. Using edge servers to cache and serve content improves performance by providing content closer to where viewers are located. CloudFront has edge servers in locations all around the world.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

Question #19

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Answer: C

Reference:

<https://medium.com/@KerrySheldon/s3-exercise-2-4-adding-objects-to-an-s3-bucket-with-cross-region-replication-a78b332b7697>

Question #20

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic

from the applications.

Which action will fulfill these requirements and maintain security?

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

Answer: *B*

Question #21

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Answer: *A*

Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of

DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections.

Applications connect to a read replica the same way they do to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #22

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Answer: AD

Question #23

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Answer: BD

Cross Region EC2 AMI Copy -

We know that you want to build applications that span AWS Regions and we're working to provide you with the services and features needed to do so. We started out by launching the EBS Snapshot Copy feature late last year. This feature gave you the ability to copy a snapshot from Region to Region with just a couple of clicks. In addition, last month we made a significant reduction (26% to 83%) in the cost of transferring data between AWS Regions, making it less expensive to operate in more than one AWS region.

Today we are introducing a new feature: Amazon Machine Image (AMI) Copy. AMI Copy enables you to easily copy your Amazon Machine Images between AWS

Regions. AMI Copy helps enable several key scenarios including:

Simple and Consistent Multi-Region Deployment " You can copy an AMI from one region to another, enabling you to easily launch consistent instances based on the same AMI into different regions.

Scalability " You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location.

Performance " You can increase performance by distributing your application and locating critical components of your application in closer proximity to your users.

You can also take advantage of region-specific features such as instance types or other AWS services.

Even Higher Availability " You can design and deploy applications across AWS regions, to increase availability.

Once the new AMI is in an Available state the copy is complete.

Reference:

<https://aws.amazon.com/blogs/aws/ec2-ami-copy-between-regions/>

Question #24

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.

What should the solutions architect do to accomplish this? (Choose two.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Answer: AB

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Gateway endpoints -

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3 -

DynamoDB -

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Question #25

A company's legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted. How should this be accomplished?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the over to the new master. Delete the old RDS instance.

Answer: C

How do I encrypt Amazon RDS snapshots?

The following steps are applicable to Amazon RDS for MySQL, Oracle, SQL Server, PostgreSQL, or MariaDB.

Important: If you use Amazon Aurora, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster if you specify an AWS Key

Management Service (AWS KMS) encryption key when you restore from the unencrypted DB cluster snapshot.

For more information, see Limitations of Amazon RDS Encrypted DB Instances.

Open the Amazon RDS console, and then choose Snapshots from the navigation pane.

Select the snapshot that you want to encrypt.

Under Snapshot Actions, choose Copy Snapshot.

Choose your Destination Region, and then enter your New DB Snapshot Identifier.

Change Enable Encryption to Yes.

Select your Master Key from the list, and then choose Copy Snapshot.

After the snapshot status is available, the Encrypted field will be True to indicate that the snapshot is encrypted.

You now have an encrypted snapshot of your DB. You can use this encrypted DB snapshot to restore the DB instance from the DB snapshot.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-rds-snapshots/>

Question #26

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.

- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Answer: A

Question #27

A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow. Which set of actions will improve website performance for users worldwide?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Answer: A

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Routing traffic to an Amazon CloudFront web distribution by using your domain name.

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website — including dynamic, static, streaming, and interactive content — by using a global network of edge locations. Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

To use CloudFront to distribute your content, you create a web distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want

CloudFront to get your content from, whether you want only selected users to have access to your content, and

whether you want to require users to use HTTPS.

When you create a web distribution, CloudFront assigns a domain name to the distribution, such as `asd111111abcdef8.cloudfront.net`. You can use this domain name in the URLs for your content, for example:

[1]

Alternatively, you might prefer to use your own domain name in URLs, for example:

[1]

If you want to use your own domain name, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. An alias record is a Route

53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as `example.com`, and for subdomains, such as `www.example.com`. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #28

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions.
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Answer: C

AWS Lambda -

With Lambda, you can run code for virtually any type of application or backend service — all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

How it works -



Amazon API Gateway -

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

Reference:

<https://aws.amazon.com/lambda/>

<https://aws.amazon.com/api-gateway/>

Question #29

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted. The company wants to minimize costs.

Which pricing model should the company choose?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances

Answer: D

Explanation -

Scheduled Reserved Instances -

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances

are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled

Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

If you require a capacity reservation on a continuous basis, Reserved Instances might meet your needs and decrease costs.

How Scheduled Instances Work -

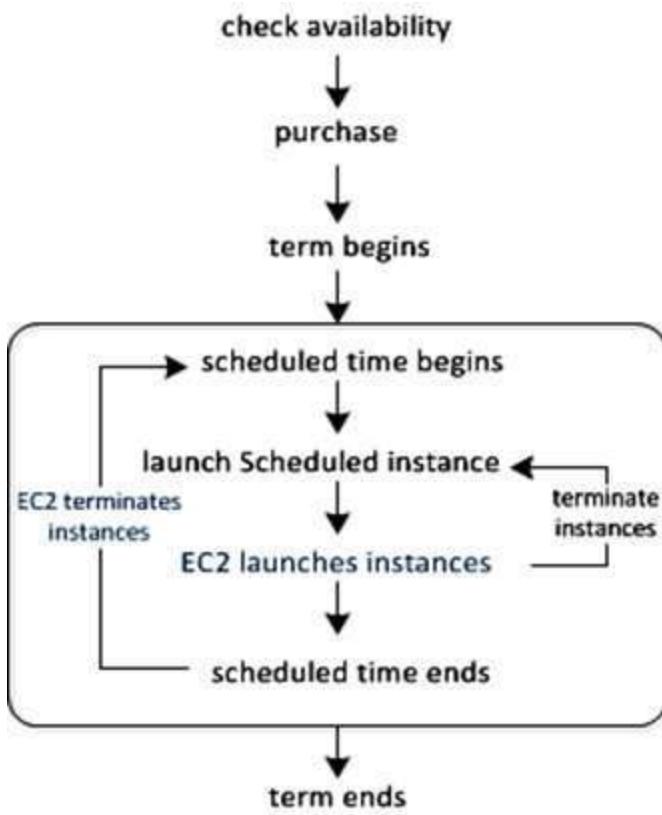
Amazon EC2 sets aside pools of EC2 instances in each Availability Zone for use as Scheduled Instances. Each pool supports a specific combination of instance type, operating system, and network.

To get started, you must search for an available schedule. You can search across multiple pools or a single pool. After you locate a suitable schedule, purchase it.

You must launch your Scheduled Instances during their scheduled time periods, using a launch configuration that matches the following attributes of the schedule that you purchased: instance type, Availability Zone, network, and platform. When you do so, Amazon EC2 launches EC2 instances on your behalf, based on the specified launch specification. Amazon EC2 must ensure that the EC2 instances have terminated by the end of the current scheduled time period so that the capacity is available for any other Scheduled Instances it is reserved for. Therefore, Amazon EC2 terminates the EC2 instances three minutes before the end of the current scheduled time period.

You can't stop or reboot Scheduled Instances, but you can terminate them manually as needed. If you terminate a Scheduled Instance before its current scheduled time period ends, you can launch it again after a few minutes. Otherwise, you must wait until the next scheduled time period.

The following diagram illustrates the lifecycle of a Scheduled Instance.



Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Question #30

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.

What should a solutions architect do to meet these requirements? (Choose two.)?

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Answer: CE

Network Load Balancer overview -

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the

port specified in the listener configuration.

When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. For more information, see Availability Zones.

If you enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone, this increases the fault tolerance of your applications. For example, if one or more target groups does not have a healthy target in an Availability Zone, we remove the IP address for the corresponding subnet from DNS, but the load balancer nodes in the other Availability Zones are still available to route traffic. If a client doesn't honor the time-to-live (TTL) and sends requests to the IP address after it is removed from DNS, the requests fail.

For TCP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, destination port, and TCP sequence number. The TCP connections from a client have different source ports and sequence numbers, and can be routed to different targets. Each individual TCP connection is routed to a single target for the life of the connection.

For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

Question #31

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.

- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Answer: C

However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

DB instances that are encrypted can't be modified to disable encryption.

You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.

Encrypted read replicas must be encrypted with the same key as the source DB instance when both are in the same AWS Region.

You can't restore an unencrypted backup or snapshot to an encrypted DB instance.

To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key identifier of the destination AWS Region. This is because KMS encryption keys are specific to the AWS Region that they are created in.

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Question #32

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Answer: C

Reference:

[\(geolocation routing\)](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Question #33

A solutions architect has created a new AWS account and must secure AWS account root user access. Which combination of actions will accomplish this? (Choose two.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Answer: AB

Question #34

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

S3 Intelligent-Tiering -

S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers – frequent access and infrequent access – when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.99999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/>

Question #35

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Answer: B

If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those IP addresses.

AWS Web Application Firewall (WAF) " Helps to protect your web applications from common application-layer exploits that can affect availability or consume excessive resources. As you can see in my post (New " AWS WAF), WAF allows you to use access control lists (ACLs), rules, and conditions that define acceptable or unacceptable requests or IP addresses. You can selectively allow or deny access to specific parts of your web application and you can also guard against various SQL injection attacks. We launched WAF with support for Amazon CloudFront.

Reference:

<https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-loadbalancers/>

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-ip-conditions.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-ip-conditions.html>

<https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-load-balancers/>

Question #36

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Answer: C

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

Question #37

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Answer: C

Working with cross-site scripting match conditions

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URL or the query string, that you want AWS WAF Classic to inspect for possible malicious scripts. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious scripts.

Web Application Firewall -

You can now use AWS WAF to protect your web applications on your Application Load Balancers. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

<https://aws.amazon.com/elasticloadbalancing/features/>

Question #38

A company's website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage. There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS

DB instance slows down significantly when the internal systems fetch data. This impacts the website's read and write performance, and the users experience slow response times.

Which solution will improve the website's performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Answer: D

Amazon RDS Read Replicas -

Enhanced performance -

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Because read replicas can be promoted to master status, they are useful as part of a sharding implementation.

To further maximize read performance, Amazon RDS for MySQL allows you to add table indexes directly to Read Replicas, without those indexes being present on the master.

Reference:

<https://aws.amazon.com/rds/features/read-replicas>

Question #39

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Answer: B

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 AutoScaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to: Configure a target tracking scaling policy to keep

the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your AutoScaling group.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Question #40

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Answer: A D

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

Question #41

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.

Which changes should be made to the database tier to improve performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
- C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Answer: D

Question #42

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution. What should a solutions architect do to accomplish this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
- D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

L

Answer: B

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price.

You incur regular Amazon S3 charges for storing the objects in the bucket.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #43

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon EBS Provisioned IOPS SSD (io1)

Answer: *B*

Explanation -

Amazon FSx for Lustre -

Amazon FSx for Lustre is a new, fully managed service provided by AWS based on the Lustre file system. Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

FSx for Lustre allows customers to create a Lustre filesystem on demand and associate it to an Amazon S3 bucket. As part of the filesystem creation, Lustre reads the objects in the buckets and adds that to the file system metadata. Any Lustre client in your VPC is then able to access the data, which gets cached on the high-speed Lustre filesystem. This is ideal for HPC workloads, because you can get the speed of an optimized Lustre file system without having to manage the complexity of deploying, optimizing, and managing the Lustre cluster. Additionally, having the filesystem work natively with Amazon S3 means you can shut down the Lustre filesystem when you don't need it but still access objects in

Amazon S3 via other AWS Services. FSx for Lustre also allows you to also write the output of your HPC job back to Amazon S3.

Reference:

https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf

(p.8)

Question #44

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.

What should the solutions architect recommend?

- A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.

- B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.
- C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Answer: A

AWS Managed Microsoft AD -

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2012 R2. When you select and launch this directory type, it is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC). The domain controllers run in different Availability Zones in a region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you.

Reference:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

Question #45

A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

- A. Enable Amazon S3 versioning.
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy.
- D. Enable Amazon S3 cross-Region replication.

Answer: A

Data can be recover if versioning enable, also it provide a extra protection like file delete,MFA delete. MFA.

Delete only works for CLI or API interaction, not in the

AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled

Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Reference:

<https://books.google.com.sg/books?id=wv45DQAAQBAJ&pg=PA39&lpg=PA39&dq=hosts+a+static+website+with+in+an+Amazon+S3+bucket.+A+solutions+architect+needs+to+ensure+that+data+can+be+recovered+in+case+of+accidental+deletion&source=bl&ots=0NolP5igY5&sig=ACfU3U3opL9Jha6jM2E18x7EcjK4rigQHQ&hl=en&sa=X&ved=2ahUKEwiS9e3yy7vpAhVx73MBHZNoDnQQ6AEwAHoECBQQAQ#v=onepage&q=hosts%20a%20static%20website%20within%20an%20Amazon%20S3%20bucket.%20A%20solutions%20architect%20needs%20to%20ensure%20that%20data%20can%20be%20recovered%20in%20case%20of%20accidental%20deletion&f=false> https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/ https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html

Question #46

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Answer: B

Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/#:~>

Question #47

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Answer: *B*

AWS Storage Gateway Hardware Appliance

Hardware Appliance -

Storage Gateway is available as a hardware appliance, adding to the existing support for VMware ESXi, Microsoft Hyper-V, and Amazon EC2. This means that you can now make use of Storage Gateway in situations where you do not have a virtualized environment, server-class hardware or IT staff with the specialized skills that are needed to manage them. You can order appliances from Amazon.com for delivery to branch offices, warehouses, and *outpost* offices that lack dedicated IT resources. Setup (as you will see in a minute) is quick and easy, and gives you access to three storage solutions:

File Gateway *"* A file interface to Amazon S3, accessible via NFS or SMB. The files are stored as S3 objects, allowing you to make use of specialized S3 features such as lifecycle management and cross-region replication. You can trigger AWS Lambda functions, run Amazon Athena queries, and use Amazon Macie to discover and classify sensitive data.

Reference:

<https://aws.amazon.com/blogs/aws/new-aws-storage-gateway-hardware-appliance/>
<https://aws.amazon.com/storagegateway/file/>

Question #48

A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

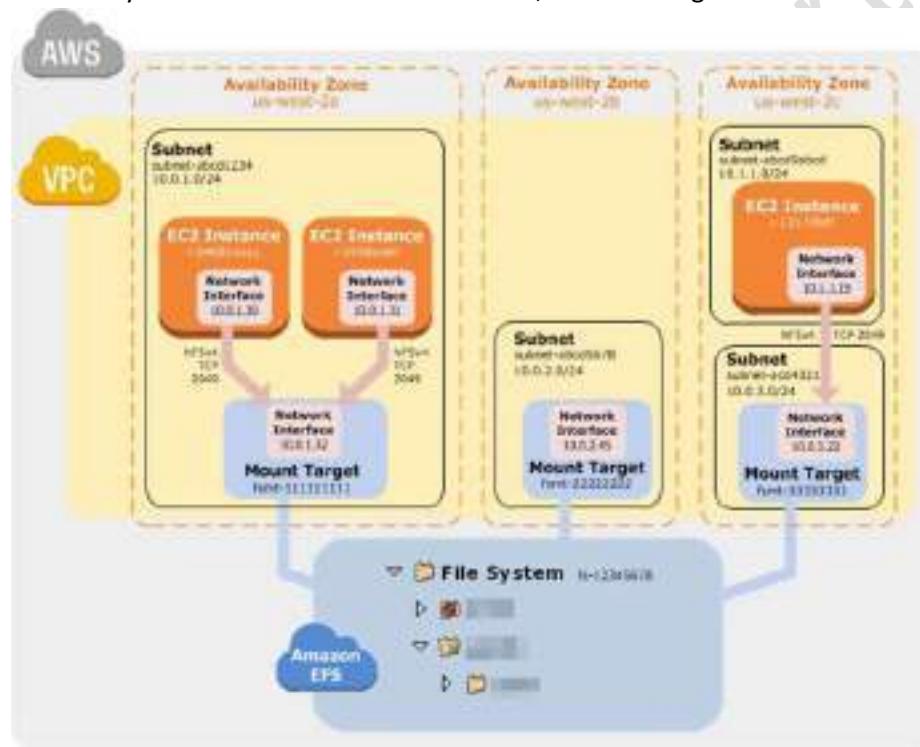
- A. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
- B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- C. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.
- D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: C

How Amazon EFS Works with Amazon EC2

The following illustration shows an example VPC accessing an Amazon EFS file system. Here, EC2 instances in the VPC have file systems mounted.

In this illustration, the VPC has three Availability Zones, and each has one mount target created in it. We recommend that you access the file system from a mount target within the same Availability Zone. One of the Availability Zones has two subnets. However, a mount target is created in only one of the subnets.



Benefits of Auto Scaling -

Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Amazon EC2 Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Amazon EC2 Auto Scaling can launch instances in another one to compensate.

Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of

capacity to handle the current traffic demand.

Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you save money by launching instances when they are needed and terminating them when they aren't.

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

Question #49

A security team to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations.

The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Answer: D

Service Control Policy concepts -

SCPs offer central access controls for all IAM entities in your accounts. You can use them to enforce the permissions you want everyone in your business to follow. Using SCPs, you can give your developers more freedom to manage their own permissions because you know they can only operate within the boundaries you define.

You create and apply SCPs through AWS Organizations. When you create an organization, AWS Organizations automatically creates a root, which forms the parent container for all the accounts in your organization. Inside the root, you can group accounts in your organization into organizational units (OUs) to simplify management of these accounts. You can create multiple OUs within a single organization, and you can create OUs within other OUs to form a hierarchical structure. You can attach SCPs to the organization root, OUs, and individual accounts. SCPs attached to the root and OUs apply to all OUs and accounts inside of them.

SCPs use the AWS Identity and Access Management (IAM) policy language; however, they do not grant permissions. SCPs enable you set permission guardrails by defining the maximum available permissions for IAM entities in an account. If a SCP denies an action for an account, none of the entities in the account can take that action, even if their IAM permissions allow them to do so. The guardrails set in SCPs apply to all IAM entities in the account, which include all users, roles, and the account root user.

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-aws-organization/>

#:<~:text=Central%20security%20administrators%20use%20service,users%20and%20roles)%20adhere%20to.&text=Now%2C%20using%20SCPs%2C%20you%

20can,your%20organization%20or%20organizational%20unit
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Question #50

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.

What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: *B*

Reference:

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

Question #51

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Answer: *C*

Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu

AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools. For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For

some AMIs, you'll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see [Installing the NFS Client](#).

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

How Amazon EFS Works with Amazon EC2

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2>

Question #52

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Answer: D

"Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom."

Server-Side Encryption: Using SSE-KMS

You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSE-S3, SSE-C, or SSE-KMS.

SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see [Protecting Data Using Server-Side](#)

Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

SSE-C requires that you manage the encryption key. For more information about SSE-C, see [Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys \(SSE-C\)](#).

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

You can request encryption and select a CMK by using the Amazon S3 console or API. In the console, check the appropriate box to perform encryption and select your CMK from the list. For the Amazon S3 API, specify encryption and choose your CMK by setting the appropriate headers in a GET or PUT request.

Reference:

<https://aws.amazon.com/kms/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

Question #53

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Answer: *D*

Reserved Instances -

Having 50 EC2 RIs provide a discounted hourly rate and an optional capacity reservation for EC2 instances. AWS Billing automatically applies your RI's discounted rate when attributes of EC2 instance usage match attributes of an active RI.

If an Availability Zone is specified, EC2 reserves capacity matching the attributes of the RI. The capacity reservation of an RI is automatically utilized by running instances matching these attributes.

You can also choose to forego the capacity reservation and purchase an RI that is scoped to a region. RIs that are scoped to a region automatically apply the RI's discount to instance usage across AZs and instance sizes in a region, making it easier for you to take advantage of the RI's discounted rate.

On-Demand Instance -

On-Demand instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

The pricing below includes the cost to run private and public AMIs on the specified operating system (Windows Usage prices apply to Windows Server 2003 R2,

2008, 2008 R2, 2012, 2012 R2, 2016, and 2019). Amazon also provides you with additional instances for Amazon EC2 running Microsoft Windows with SQL

Server, Amazon EC2 running SUSE Linux Enterprise Server, Amazon EC2 running Red Hat Enterprise Linux and Amazon EC2 running IBM that are priced differently.

Spot Instances -

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in

each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

<https://aws.amazon.com/ec2/pricing/on-demand/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

Question #54

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

- A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.
- B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
- C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.
- E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Answer: DE

Question #55

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection.

What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket policy to enforce a VPC endpoint.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Answer: D

Regional Limitations for AWS Snowball

The AWS Snowball service has two device types, the standard Snowball and the Snowball Edge. The following table highlights which of these devices are available in which regions.

Region	Snowball Availability	Snowball Edge Availability
US East (Ohio)	50 TB and 80 TB	100 TB
US East (N. Virginia)	50 TB and 80 TB	100 TB
US West (N. California)	50 TB and 80 TB	100 TB
US West (Oregon)	50 TB and 80 TB	100 TB
Canada (Central)	80 TB only	100 TB
Asia Pacific (Mumbai)	80 TB only	100 TB
Asia Pacific (Singapore)	80 TB only	100 TB
Asia Pacific (Sydney)	80 TB only	100 TB
Asia Pacific (Tokyo)	80 TB only	100 TB
EU (Frankfurt)	80 TB only	100 TB
EU (Ireland)	80 TB only	100 TB
EU (London)	80 TB only	100 TB
South America (São Paulo)	80 TB only	100 TB

Limitations on Jobs in AWS Snowball

The following limitations exist for creating jobs in AWS Snowball:

For security purposes, data transfers must be completed within 90 days of the Snowball being prepared.

Currently, AWS Snowball Edge device doesn't support server-side encryption with customer-provided keys (SSE-C). AWS Snowball Edge device does support server-side encryption with Amazon S3's managed encryption keys (SSE-S3) and server-side encryption with AWS Key Management Service's managed keys (SSE-KMS). For more information, see Protecting Data Using Server-Side Encryption in the Amazon Simple Storage Service Developer Guide.

In the US regions, Snowballs come in two sizes: 50 TB and 80 TB. All other regions have the 80 TB Snowballs only. If you're using Snowball to import data, and you need to transfer more data than will fit on a single Snowball, create additional jobs. Each export job can use multiple Snowballs.

The default service limit for the number of Snowballs you can have at one time is 1. If you want to increase your service limit, contact AWS Support.

All objects transferred to the Snowball have their metadata changed. The only metadata that remains the same is filename and filesize. All other metadata is set as in the following example: -rw-rw-r-- 1 root root [filesize] Dec

31 1969 [path/filename].

Object lifecycle management -

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions – Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions – Define when objects expire. Amazon S3 deletes expired objects on your behalf.

The lifecycle expiration costs depend on when you choose to expire objects.

Reference:

<https://docs.aws.amazon.com/snowball/latest/ug/limits.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

Question #56

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet. The web application instances and the database are running in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Choose two.)

- A. Create new public and private subnets in the same AZ for high availability.
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.
- E. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Answer: *BE*

Question #57

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.

E. Encrypt the bucket using AWS KMS

Answer: *BD*

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

To customize your data retention approach and control storage costs, use object versioning with Object lifecycle management. For information about creating S3

Lifecycle policies using the AWS Management Console, see How Do I Create a Lifecycle Policy for an S3 Bucket? in the Amazon Simple Storage Service Console

User Guide.

If you have an object expiration lifecycle policy in your non-versioned bucket and you want to maintain the same permanent delete behavior when you enable versioning, you must add a noncurrent expiration policy. The noncurrent expiration lifecycle policy will manage the deletes of the noncurrent object versions in the version-enabled bucket. (A version-enabled bucket maintains one current and zero or more noncurrent object versions.) You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Enabling and suspending versioning is done at the bucket level. When you enable versioning on an existing bucket, objects that are already stored in the bucket are unchanged. The version IDs (null), contents, and permissions remain the same. After you enable S3 Versioning for a bucket, each object that is added to the bucket gets a version ID, which distinguishes it from other versions of the same key.

Only Amazon S3 generates version IDs, and they can't be edited. Version IDs are Unicode, UTF-8 encoded, URL-ready, opaque strings that are no more than

1,024 bytes long. The following is an example:

3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCx3vjVBH40Nr8X8gdRQBpUMLUo.

Using MFA delete -

If a bucket's versioning configuration is MFA Delete-enabled, the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket. Requests that include x-amz-mfa must use HTTPS. The header's value is the concatenation of your authentication device's serial number, a space, and the authentication code displayed on it. If you do not include this request header, the request fails.

Reference:

<https://aws.amazon.com/s3/features/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Question #58

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in

size. The application owner will make the log file available to the vendor for a limited time. What is the MOST secure way to do this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Answer: C

Share an object with others -

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method

(GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.

Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

Question #59

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Answer: AC

Question #60

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM activity across all account in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Answer: D

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Question #61

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an

Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Answer: B

Expanding Your Scaled and Load-Balanced Application to an Additional Availability Zone.

When one Availability Zone becomes unhealthy or unavailable, Amazon EC2 Auto Scaling launches new instances in an unaffected zone. When the unhealthy

Availability Zone returns to a healthy state, Amazon EC2 Auto Scaling automatically redistributes the application instances evenly across all of the zones for your

Auto Scaling group. Amazon EC2 Auto Scaling does this by attempting to launch new instances in the Availability Zone with the fewest instances. If the attempt fails, however, Amazon EC2 Auto Scaling attempts to launch in other Availability Zones until it succeeds.

You can expand the availability of your scaled and load-balanced application by adding an Availability Zone to your Auto Scaling group and then enabling that zone for your load balancer. After you've enabled the new Availability Zone, the load balancer begins to route traffic equally among all the enabled zones.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

Question #62

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.

Which storage service should a solutions architect use to provide the MOST cost-effective solution?

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon EC2 instance store
- D. Amazon S3

Answer: D

Amazon S3 -

Requests to Amazon S3 can be authenticated or anonymous. Authenticated access requires credentials that AWS can use to authenticate your requests. When making REST API calls directly from your code, you create a signature using valid credentials and include the signature in your request. Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Reference:

<https://aws.amazon.com/s3/>

Question #63

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL.
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Answer: C

In-memory databases on AWS Amazon ElastiCache for Redis.

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides submillisecond latency to power internet-scale, real-time applications.

Developers can use ElastiCache for Redis as an in-memory nonrelational database. The ElastiCache for Redis

cluster configuration supports up to 15 shards and enables customers to run Redis workloads with up to 6.1 TB of in-memory capacity in a single cluster. ElastiCache for Redis also provides the ability to add and remove shards from a running cluster. You can dynamically scaleout and even scale in your Redis cluster workloads to adapt to changes in demand.

Reference:

<https://aws.amazon.com/elasticsearch/redis/faqs/>

<https://aws.amazon.com/nosql/in-memory/>

Question #64

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an

Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.

What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Answer: A

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined — such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

As an example, suppose that you're serving an image from a traditional web server, not from CloudFront. For example, you might serve an image,

[1]

Your users can easily navigate to this URL and see the image. But they probably don't know that their request was routed from one network to another — through the complex collection of interconnected networks that comprise the internet — until the image was found.

CloudFront speeds up the distribution of your content by routing each user request through the AWS backbone network to the edge location that can best serve your content. Typically, this is a CloudFront edge server that provides the fastest delivery to the viewer. Using the AWS network dramatically reduces the number of networks that your users' requests must pass through, which improves performance. Users get lower latency —

the time it takes to load the first byte of the file " and higher data transfer rates. You also get increased reliability and availability because copies of your files (also known as objects) are now held (or cached) in multiple edge locations around the world.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #65

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Answer: C

Amazon Simple Queue Service -

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

Scaling Based on Amazon SQS -

There are some scenarios where you might think about scaling in response to activity in an Amazon SQS queue. For example, suppose that you have a web app that lets users upload images and use them online. In this scenario, each image requires resizing and encoding before it can be published. The app runs on EC2 instances in an Auto Scaling group, and it's configured to handle your typical upload rates. Unhealthy instances are terminated and replaced to maintain current instance levels at all times. The app places the raw bitmap data of the images in an SQS queue for processing. It processes the images and then publishes the processed images where they can be viewed by users. The architecture for this scenario works well if the number of image uploads doesn't vary over time. But if the number of uploads changes over time, you might consider using dynamic scaling to scale the capacity of your Auto Scaling group.

Reference:

<https://aws.amazon.com/sqs/#:~:text=Amazon%20SQS%20leverages%20the%20AWS,queues%20provide%20near%20unlimited%20throughput> <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Question #66

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
- D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

Answer: C

Question #67

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow.

Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Answer: A

Reference:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

Question #68

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application's history the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Answer: B

Question #69

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon

RDS table, and deletes -

the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Answer: D

Question #70

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

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

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Answer: C

Question #71

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

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

Answer: A

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

Question #72

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the

MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Answer: D

Question #73

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Answer: D

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Question #74

A company built a food ordering application that captures user data and stores it for future analysis. The application's static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

- A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Answer: D

Question #75

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Answer: B

Question #76

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be

accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Answer: *D*

Reference:

<https://aws.amazon.com/kinesis/data-analytics/>

Question #77

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

Answer: *B*

Question #78

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.
- C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.

D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

Answer: *B*

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

Question #79

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Answer: *A*

Explanation:

Keyword: Move existing data and support future records + Granular audit access at all levels

Use AWS DataSync to migrate existing data to Amazon S3, and then use the File Gateway configuration of AWS Storage Gateway to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.

Need a solution to move existing data and support future records = AWS DataSync should be used for migration.

Need granular audit access at all levels = Data Events should be used in CloudTrail, Management Events is enabled by default.

CORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events" is the correct answer.

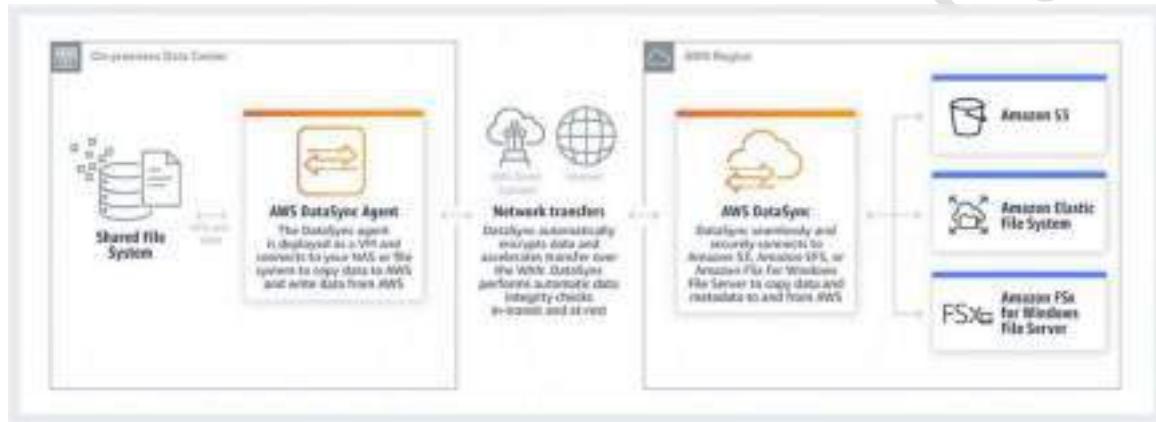
INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events" is incorrect as "current infrastructure is running out of space"

INCORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events." is incorrect as "Management Events is enabled by default"

INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use AmazonElastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and

enable Amazon S3 server access logging." is incorrect as "current infrastructure is running out of space"

How AWS DataSync Works



How AWS CloudTrail works



References:

<https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

<https://aws.amazon.com/cloudtrail/>

<https://aws.amazon.com/storagegateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Question #80

A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution's cost should be minimal.

Which storage solution meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: D

Question #81

A company's operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.

Which solution would satisfy these requirements?

- A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.
- B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.
- C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
- D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

Answer: D

Question #82

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Answer: A

Question #83

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences. The application is successful with a rapid increase in the number of users every month.

The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon

RDS for MySQL instance has triggered alarms related to resource exhaustion due to read requests.

What can a solutions architect recommend to prevent service interruptions at the database layer with minimal changes to code?

- A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.
- B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

Answer: A

Question #84

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

\

Answer: A

Question #85

A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.

Which solution should a solutions architect recommend that is MOST highly available?

- A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
- B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
- C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
- D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Answer: C

Question #86

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.

What should a solutions architect recommend?

- A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.
- D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Answer: A

Question #87

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Execute a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Answer: B

Question #88

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

Which solution should a solutions architect recommend to keep the data private?

- A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Answer: A

Question #89

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Answer: B

Question #90

A public-facing web application queries a database hosted on an Amazon EC2 instance in a private subnet. A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.
What should a solutions architect recommend to the application team? (Choose two.)

- A. Cache query data in Amazon SQS
- B. Create a read replica to offload queries
- C. Migrate the database to Amazon Athena
- D. Implement Amazon DynamoDB Accelerator to cache data.
- E. Migrate the database to Amazon RDS

Answer: *BE*

Question #91

A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

- A. Add a rule in the inbound table of the security group to deny the traffic from that CIDR range.
- B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
- C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
- D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Answer: *C*

Question #92

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on

Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability to shift traffic from resources in one region to another.

What should a solutions architect recommend?

- A. Configure an Amazon Route 53 latency routing policy.
- B. Configure an Amazon Route 53 geolocation routing policy.
- C. Configure an Amazon Route 53 geoproximity routing policy.
- D. Configure an Amazon Route 53 multivalue answer routing policy.

Answer: *C*

Question #93

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share.

Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.

What should a solutions architect recommend to meet these requirements?

- A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.
- B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.
- C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
- D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Answer: *D*

Question #94

An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.

Which solution is the MOST cost-effective?

- A. DEV with Spot Instances and PROD with On-Demand Instances
- B. DEV with On-Demand Instances and PROD with Spot Instances
- C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
- D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Answer: *C*

Question #95

A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage.

How can this be achieved?

- A. Create an Amazon EFS file system and mount it from each EC2 instance.
- B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.
- C. Create a file system on an Amazon EBS Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.
- D. Create file systems on Amazon EBS volumes attached to each EC2 instance. Synchronize the Amazon EBS volumes across the different EC2 instances.

Answer: *A*

Question #96

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Answer: C

Question #97

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.

Which of the following would be the LEAST complicated implementation?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Answer: C

Question #98

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.

Which database implementations will meet these requirements? (Choose two.)

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon RDS for MySQL
- D. MySQL-compatible Amazon Aurora Multi-AZ
- E. Amazon RDS for SQL Server Standard Edition Multi-AZ

Answer: DE

Question #99

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only. Which configuration will meet this requirement?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Answer: C

Reference:

<https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/>

Question #100

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

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

Answer: C

Question #101

A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates. The company does not want external websites to see the EC2 instance IP address or initiate connections to it.

How can a solutions architect achieve this objective?

- A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
- B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
- C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
- D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

Answer: B

Question #102

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

Answer: A

Question #103

A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

- A. Use step scaling.
- B. Use simple scaling.
- C. Use lifecycle hooks.
- D. Use scheduled scaling.

Answer: D

Question #104

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Answer: B

Question #105

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data

at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
- C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
- D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Answer: **B**

Question #106

A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis.

What is the MOST cost-effective storage solution alternative to the current configuration?

- A. Configure a lifecycle policy to delete the objects after 30 days.
- B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
- C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: **D**

Question #107

A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited time. What should a solutions architect do to securely meet these requirements?

- A. Enable public access on an Amazon S3 bucket.
- B. Generate a presigned URL to share with the users.
- C. Encrypt files using AWS KMS and provide keys to the users.
- D. Create and assign IAM roles that will grant GetObject permissions to the users.

Answer: **B**

Question #108

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an

NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing. Which solution will meet these requirements?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
- B. Use an AWS storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

Answer: A

Reference:

<https://aws.amazon.com/storagegateway/file/>

Question #109

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon S3.

What should a solutions architect recommend to satisfy these requirements?

- A. Server-side encryption with customer-provided encryption keys
- B. Client-side encryption with Amazon S3 managed encryption keys
- C. Server-side encryption with keys stored in AWS Key Management Service (AWS KMS)
- D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Answer: D

Question #110

A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted. Which combination of steps will meet these requirements? (Choose two.)

- A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
- B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
- C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
- D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.

E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

Answer: AB

Question #111

A company is investigating potential solutions that would collect, process, and store users' service usage data. The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.

Which solution should a solutions architect recommend?

- A. Use Amazon DynamoDB transactions.
- B. Create an Amazon Neptune database in a Multi-AZ design
- C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.
- D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon EBS Throughput Optimized HDD (st1) storage.

Answer: C

Question #112

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.

How should a solutions architect optimize high availability for the application?

- A. Use Lambda@Edge for CloudFront.
- B. Use Amazon S3 Transfer Acceleration for CloudFront.
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Answer: C

Question #113

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate AWS accounts. The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

Answer: A

Question #114

A company currently stores symmetric encryption keys in a hardware security module (HSM). A solutions architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys.

Where should the key material be stored to meet these requirements?

- A. Amazon S3
- B. AWS Secrets Manager
- C. AWS Systems Manager Parameter store
- D. AWS Key Management Service (AWS KMS)

Answer: D

Question #115

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Answer: D

Question #116

A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.

Which solution should the solutions architect recommend?

- A. Amazon EBS Cold HDD (sc1)
- B. Amazon EBS General Purpose SSD (gp2)
- C. Amazon EBS Provisioned IOPS SSD (io1)

D. Amazon EBS Throughput Optimized HDD (st1)

Answer: *B*

Question #117

A company's application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet.

How should a solutions architect configure access?

- A. Create a private hosted zone using Amazon Route 53.
- B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
- C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.
- D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Answer: *B*

Question #118

A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low latency.

Which architecture should a solutions architect recommend for this situation?

- A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.
- B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.
- C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
- D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

Answer: *D*

Question #119

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer: C

Question #120

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest. Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Answer: D

Question #121

A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a Microsoft SQL Server database with heavy read activity. The company wants to explore alternate database options and migrate database engines, if needed.

Every 4 hours, the development team does a full copy of the production database to populate a test database. During this period, users experience latency.

What should a solutions architect recommend as replacement database?

- A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
- B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
- D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Answer: D

Question #122

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized. How should a solutions architect meet these requirements?

- A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
- C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

Answer: C

Question #123

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company's legacy on-premises environments and with AWS.
Which services meet the business requirements? (Choose two.)

- A. Amazon EBS
- B. Amazon EFS
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Answer: CE

Question #124

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.

Which solution will accomplish this?

- A. Spot Fleet
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

Answer: A

Question #125

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances.

What should a solutions architect do to accomplish this?

- A. Configure a volume using Amazon EFS. Mount the EFS volume to each Windows instance.
- B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.
- C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.
- D. Configure an Amazon EBS volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Answer: C

Question #126

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an

Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region.

What should a solutions architect do to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check.
- C. Create an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Question #127

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.

Which method should the solutions architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Answer: A

Reference:

<https://itexamcertified.com/>

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-accelerator-dax-in-memory-caching-for-read-intensive-workloads/>

Question #128

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company's architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group.
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica.
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Answer: C

Question #129

A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function's IAM role, giving it access to put, update, and delete items in the Books table. The IAM policy must prevent function from performing any other actions on the Books table or any other.

Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": [
                "dynamodb: PutItem",
                "dynamodb: UpdateItem",
                "dynamodb: DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}
```

B.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": [
                "dynamodb: PutItem",
                "dynamodb: UpdateItem",
                "dynamodb: DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"
        }
    ]
}
```

C.

<https://itexamcertified.com/>

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}
```

D.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        },
        {
            "Sid": "PutUpdateDeleteOnBooks",
            "Effect": "Deny",
            "Action": "dynamodb:*,*",
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
        }
    ]
}
```

Answer: A

Question #130

A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company's AWS costs.

What should a solutions architect do to reduce costs?

- A. Configure Amazon CloudFront with the existing website as the origin.
- B. Move the website to Amazon EC2 with Amazon EBS volumes for storage.
- C. Use AWS Global Accelerator and specify the existing website as the endpoint.
- D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Answer: A

Question #131

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.

How should the company deploy this solution?

- A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
- B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
- D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Answer: A

Question #132

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible

I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

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

Answer: AD

Question #133

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 buckets it uses to store data. Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage.

Which solution will lower costs without compromising the availability of objects?

- A. Use S3 ACLs.
- B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.
- C. Use S3 Intelligent-Tiering storage.
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: C

Question #134

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket. The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.

Which combination of actions should solutions archived take to accomplish this? (Choose two.)

- A. Create a VPC endpoint for Amazon S3.
- B. Enable server access logging on the bucket.

- C. Apply a bucket policy to restrict access to the S3 endpoint.
- D. Add an S3 ACL to the bucket that has sensitive information.
- E. Restrict users using the IAM policy to use the specific bucket.

Answer: AC

Question #135

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.

How can a solutions architect make the system more responsive?

- A. Use Amazon SQS with AWS Lambda to generate reports.
- B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
- C. Update the client-side application code to increase its request timeout to 5 minutes.
- D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Answer: A

Question #136

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.

What should the solutions architect do to meet these requirements?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Answer: D

Question #137

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.

Which action will be MOST effective in accomplishing this?

- A. Replace the SQS queue with Amazon Kinesis Data Firehose.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.

- C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
- D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Answer: D

Question #138

A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads.

The application is critical to the business and must be highly available.

Which solution will meet these requirements?

- A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.
- B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.
- C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.
- D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

Answer: C

Question #139

A solutions architect must design a solution for a persistent database that is being migrated from on-premises to AWS. The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.

Which solution effectively meets the database administrator's criteria?

- A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
- B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
- C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
- D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Answer: B

Question #140

A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

- A. An Auto Scaling group with Spot Instance types.
- B. A placement group using a cluster placement strategy.
- C. A placement group using a partition placement strategy.
- D. An Auto Scaling group with On-Demand instance types.

Answer: *B*

Question #141

A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet. What should a solutions architect recommend to reduce internet latency?

- A. Set up AWS Global Accelerator and add endpoints.
- B. Set up AWS Direct Connect locations in multiple Regions.
- C. Set up an Amazon CloudFront distribution to access an application.
- D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Answer: *A*

Question #142

A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.

The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.

Which services satisfies these security requirements?

- A. AWS CloudHSM with the CloudHSM client
- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Answer: *A*

Question #143

A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.

Which solution meets these requirements?

- A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.
- D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

Answer: A

Question #144

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Answer: A

Question #145

A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost-effective.

Which combination of AWS services and features should the solutions architect use? (Choose two.)

- A. Amazon S3
- B. Amazon EC2
- C. AWS Fargate
- D. Amazon CloudFront
- E. Elastic Load Balancer

Answer: AD

Question #146

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

- A. Amazon EBS
- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Answer: C

Question #147

A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours.

Which solutions can accomplish this? (Choose two.)

- A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
- B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
- C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
- D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
- E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

Answer: AD

Question #148

A company has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-1 Region. A solutions architect is designing a disaster recovery strategy to have the database provisioned in the us-west-2 Region in case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

- A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.

- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
- D. Create a multimaster read/write instances across multiple AWS Regions. Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Answer: A

Question #149

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.

What would allow for automatic recovery of the EC2 instance as quickly as possible?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Answer: A

Question #150

A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center.

The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.

What should the solutions architect do to meet these requirements?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS)
- C. Set up AWS Storage Gateway as a volume gateway
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Answer: A

Question #151

A solutions architect is designing a hybrid application using the AWS cloud. The network between the on-premises data center and AWS will use an AWS Direct

Connect (DX) connection. The application connectivity between AWS and the on-premises data center must be highly resilient.

Which DX configuration should be implemented to meet these requirements?

- A. Configure a DX connection with a VPN on top of it.
- B. Configure DX connections at multiple DX locations.
- C. Configure a DX connection using the most reliable DX partner.
- D. Configure multiple virtual interfaces on top of a DX connection.

Answer: **B**

Question #152

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.

Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

- A. Deploy a NAT instance in a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Answer: **B**

Question #153

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon

RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running.

The business reporting users must be able to generate reports without affecting the application's performance.

Which action will accomplish this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Answer: **D**

Question #154

A company is running a two-tier ecommerce website using services. The current architect uses a publish-facing Elastic Load Balancer that sends traffic to Amazon

EC2 instances in a private subnet. The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MySQL database. The application is running in the United States. The company recently started selling to users in Europe and Australia. A solutions architect needs to design solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances.
- D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Answer: B

Question #155

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Answer: A

Question #156

A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server databases running on Amazon EC2 instances with

Windows Server 2016. The solution must be able to be integrated into the corporate Active Directory domain, be highly durable, be managed by AWS, and provide high levels of throughput and IOPS.

Which solution meets these requirements?

- A. Use Amazon FSx for Windows File Server.
- B. Use Amazon Elastic File System (Amazon EFS).
- C. Use AWS Storage Gateway in file gateway mode.
- D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Answer: A

Question #157

A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions. The company wants to create an allow list for the IPs of all the load balancers on its firewall device. A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall.

What should the solutions architect recommend to meet these requirements?

- A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IPs. Register the private IPs of all the ALBs as targets to this NLB.
- C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.
- D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

Answer: C

Question #158

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Answer: B

Question #159

A company is planning to migrate its virtual server-based workloads to AWS. The company has internet-facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository. Which services should a solutions architect recommend be hosted on the public subnet? (Choose two.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Answer: AC

Question #160

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Answer: *B*

Question #161

A company is using a tape backup solution to store its key application data offsite. The daily data volume is around 50 TB. The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed, and a week's notice is typically given if a backup needs to be restored.

The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes. The company also wants to make sure that the transition from tape backups to the cloud minimizes disruptions. Which storage solution is MOST cost-effective?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

Answer: *A*

Question #162

A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead.

Which solution should the solutions architect implement?

- A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.
- B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
- C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
- D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Answer: A

Question #163

A company decides to migrate its three-tier web application from on-premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.

Which AWS service meets these requirements?

- A. Amazon Aurora
- B. Amazon RDS for SqlServer
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB on-demand

Answer: A

Question #164

A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.

Which method should a solutions architect implement to meet this requirement?

- A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs.
- B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs.
- C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs.
- D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

Answer: D

Question #165

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross-communication. A recent increase in account creations and

VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs.

There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked

with creating a centrally managed networking setup for multiple accounts, VPCs, and VPNs.

Which networking solution meets these requirements?

- A. Configure shared VPCs and VPNs and share to each other.
- B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect connection between all VPCs and VPNs.

D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

Answer: D

Question #166

A solutions architect is helping a developer design a new ecommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the ecommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.

Which database solution meets these requirements?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Answer: B

Question #167

A solutions architect must migrate a Windows internet information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file Share to Amazon RDS.
- B. Migrate the file Share to AWS Storage Gateway
- C. Migrate the file Share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Answer: C

Question #168

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Answer: A

Question #169

A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.

If an Availability Zone fails, how can the company remain compliant with the SLA?

- A. Add a target tracking scaling policy with a short cooldown period.
- B. Change the Auto Scaling group launch configuration to use a larger instance type.
- C. Change the Auto Scaling group to use six servers across three Availability Zones.
- D. Change the Auto Scaling group to use eight servers across two Availability Zones.

Answer: A

Question #170

A company is reviewing its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization. A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

- A. Enable AWS Config service with the appropriate rules
- B. Enable AWS Trusted Advisor with the appropriate checks.
- C. Write a script using an AWS SDK to generate a bucket report
- D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Answer: A

Question #171

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency.

What should a solutions architect recommend to meet these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.
- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Answer: *B*

Question #172

A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain.

Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).
- B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

Answer: *D*

Question #173

A solutions architect has configured the following IAM policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "lambda:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "lambda:CreateFunction",  
                "lambda>DeleteFunction"  
            ],  
            "Resource": "*"  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "220.100.16.0/20"  
                }  
            }  
        }  
    ]  
}
```

Which action will be allowed by the policy?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

Answer: C

Question #174

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files. Which storage option meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)

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

Answer: *B*

Question #175

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

A. Move static assets to Amazon CloudFront. Leave the application in EC2 in an Auto Scaling group. Move the database to Amazon RDS to deploy Multi-AZ.

B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.

C. Move static assets to Amazon S3. Move the application to AWS Lambda with the concurrency limit set. Move the database to Amazon DynamoDB with on-demand enabled.

D. Move static assets to Amazon S3. Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled. Move the database to Amazon RDS to deploy Multi-AZ.

Answer: *B*

Question #176

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content. This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

A. Change the EBS volume to Provisioned IOPS (PIOPS).

B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.

C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.

D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Answer: *B*

Question #177

A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.

- B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
- D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
- E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Answer: AC

Question #178

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists. The company is looking for a native, software-based AWS service to accomplish this goal.
What should a solutions architect recommend as a solution?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Answer: A

Question #179

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.
What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

Answer: C

Question #180

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express framework.

Answer: *B*

Question #181

A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and

JavaScript.

Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Choose two.)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Answer: *DE*

Question #182

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only.

What should a solutions architect do to protect against data loss? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Answer: *AE*

Question #183

An operations team has a standard that states IAM policies should not be applied directly to users. Some new team members have not been following this standard. The operations manager needs a way to easily identify the users with attached policies.

What should a solutions architect do to accomplish this?

- A. Monitor using AWS CloudTrail.
- B. Create an AWS Config rule to run daily.
- C. Publish IAM user changes to Amazon SNS.
- D. Run AWS Lambda when a user is modified.

Answer: C

Question #184

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure. The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection. A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.

Which solution should the solutions architect select?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Answer: C

Question #185

A company is building applications in containers. The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS. Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software.

Which solution meets these requirements?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.
- C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

Answer: B

Question #186

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling. Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy.

Answer: D

Question #187

A solutions architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The solutions architect must improve the security posture and minimize the impact of a DDoS attack on resources.

Which solution is MOST effective?

- A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.
- B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
- C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda function that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
- D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

Answer: A

Question #188

A company has multiple AWS accounts for various departments. One of the departments wants to share an Amazon S3 bucket with all other departments.

Which solution will require the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket.
- B. Create a pre-signed URL for the bucket and share it with other departments.
- C. Set the S3 bucket policy to allow cross-account access to other departments.
- D. Create IAM users for each of the departments and configure a read-only IAM policy.

Answer: C

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

Question #189

A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.

Which action should be taken to share the S3 bucket?

- A. Update the bucket to be a Requester Pays bucket.
- B. Update the bucket to enable cross-origin resource sharing (CORS).
- C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.
- D. Create an IAM policy to require users to grant bucket-owner-full-control when uploading objects.

Answer: C

By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. To get access to the object, the object owner must explicitly grant you (the bucket owner) access. The object owner can grant the bucket owner full control of the object by updating the access control list (ACL) of the object. The object owner can update the ACL either during a put or copy operation, or after the object is added to the bucket.

Similar:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-require-object-ownership/>

Resolution Add a bucket policy that grants users access to put objects in your bucket only when they grant you (the bucket owner) full control of the object.

Reference:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-bucket-owner-access/>

Question #190

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Answer: B

Question #191

A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company's weather forecasting applications are based in a single Region and analyze the data daily.

What is the FASTEST way to aggregate data from all of these global sites?

- A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
- B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon EBS volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

Answer: B

Step-1: To transfer to S3 from global sites: Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's™ globally distributed AWS Edge Locations. Used to accelerate object uploads to S3 over long distances (latency). Transfer acceleration is as secure as a direct upload to S3.

Step-2: When the application analyze/aggregate the data from S3 and then again upload the results - Multipart upload Reference:

<http://lavnish.blogspot.com/2017/06/aws-s3-cross-region-replication.html> <https://aws.amazon.com/s3/transfer-acceleration/>

Question #192

A company has a custom application running on an Amazon EC instance that:

- ↳ Reads a large amount of data from Amazon S3
- ↳ Performs a multi-stage analysis
- ↳ Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis. The process performance depends on the temporary storage performance.

What would be the fastest storage option for holding the temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.
- B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Answer: A

Question #193

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size. Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Answer: B

Question #194

A company recently released a new type of internet-connected sensor. The company is expecting to sell thousands of sensors, which are designed to stream high volumes of data each second to a central location. A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real time with millisecond responsiveness.

Which solution should the solutions architect recommend?

- A. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- B. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
- C. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Answer: D

Question #195

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.

How should a solutions architect redesign the architecture to better respond to changing traffic?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Answer: D

Question #196

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company's application. A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.

What should the solutions architect recommend?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Answer: C

Question #197

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Answer: B

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

Question #198

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

443.

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

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Answer: AE

Question #199

A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for a minimum of two instances and a maximum of four instances across two Availability Zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for all the EC2 instances.

What should the solutions architect recommend to maximize utilization while ensuring the application remains fault tolerant?

- A. Remove some EC2 instances to increase the utilization of remaining instances.
- B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
- C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
- D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

Answer: D

As the Launch Configuration cannot be modified once created, the only way to update the Launch Configuration for an Auto Scaling group is to create a new one and associate it with the Auto Scaling group.

Question #200

A company has an application that posts messages to Amazon SQS. Another application polls the queue and processes the messages in an I/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages, the company has difficulty meeting its SLA consistently.

What should a solutions architect do to help improve the application's processing time and ensure it can handle the load at any level?

- A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.
- B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance.
- C. Create an Amazon Machine image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy to keep its aggregate CPU utilization below 70%.

D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

Answer: D

Question #201

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Answer: A

Question #202

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

Answer: B

Question #203

A company's packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to further reduce data transfer costs. The company cannot modify the application's source code.

What should a solutions architect do to reduce costs?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.

- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Answer: A

Question #204

A database is on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that experiences highly dynamic reads. Application developers notice a significant slowdown when testing read performance from a secondary AWS Region. The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

- A. Install MySQL on Amazon EC2 in the secondary Region.
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary Region.
- D. Implement Amazon ElastiCache to improve database query performance.

Answer: B

Reference:

<https://aws.amazon.com/rds/aurora/global-database/>

Question #205

A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days.

Which solution should a solutions architect recommend?

- A. Set the backup retention period to 90 days when creating the RDS DB instance.
- B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.
- C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days. Create an AWS Backup job to schedule the execution of the backup plan daily.
- D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot. Purge snapshots older than 90 days.

Answer: C

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

Question #206

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor's proprietary format. Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the

files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation.

What should a solutions architect do to accomplish this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.
- D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

Answer: D

Question #207

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority. Which instance type should a solutions architect recommend for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Answer: A

Question #208

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Answer: D

Reference:

<https://aws.amazon.com/fsx/windows/>

Question #209

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Answer: B

Question #210

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Answer: B

Question #211

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

- A. Place all the EC2 instances in an Auto Scaling group.
- B. Place all the EC2 instances in the same AWS Region.
- C. Place all the EC2 instances in the same Availability Zone.

D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Answer: B

Question #212

A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.

What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

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

Answer: D

Question #213

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Answer: B

Reference:

<https://aws.amazon.com/blogs/aws/protect-web-sites-services-using-rate-based-rules-for-aws-waf/>

Question #214

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.

What should the solutions architect recommend to build the MOST high-performing solution?

- A. Use AWS Glue to process data and Amazon S3 to store data.
- B. Use Amazon EMR to process data and Amazon Redshift to store data.
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

Answer: B

Reference:

<https://aws.amazon.com/redshift/features/>

Question #215

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website's ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

- A. Launch an Amazon ElastiCache cluster to cache common database queries.
- B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
- C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.
- D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

Answer: B

Question #216

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends. A solutions architect needs to design a cost-effective solution that can handle the load.

What should the solutions architect do to meet these requirements?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable Multi-AZ replication for the DynamoDB database.
- C. Enable DynamoDB auto scaling when creating the tables.
- D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Answer: C

Question #217

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

- A. Enable concurrency scaling.
- B. Enable cross-Region snapshots.
- C. Increase the data retention period.
- D. Deploy Amazon Redshift in Multi-AZ.

Answer: B

Question #218

A company has data stored in an on-premises data center that is used by several on-premises applications. The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

- A. Amazon Redshift
- B. AWS Storage Gateway for files
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Answer: B

Question #219

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Answer: D

Question #220

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company's needs and takes the LEAST amount of time?

- A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.
- B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.
- C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.
- D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

Answer: D

Question #221

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Answer: A

Question #222

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.

What should a solutions architect recommend?

- A. Set up a new Direct Connect connection in another AWS Region.
- B. Set up a new AWS managed VPN connection in another AWS Region.
- C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
- D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

Answer: C

Question #223

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

Answer: A

Question #224

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Answer: B

Question #225

A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short

Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.

What should a solutions architect recommend?

- A. Use Amazon DynamoDB global tables.
- B. Use Amazon Aurora Global Database.
- C. Use Amazon RDS for MySQL with a cross-Region read replica.
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

Answer: A

Question #226

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Answer: AE

Question #227

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.

Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

- A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
- B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
- C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
- D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

Answer: A

Question #228

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on

Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored. The amount of data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1 TB.

Which storage solution should the solutions architect recommend?

- A. An Amazon DynamoDB table accessible by all ECS cluster instances.
- B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
- C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
- D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

Answer: C

Question #229

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.

Which configuration should a solutions architect recommend?

- A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.
- B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.
- C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
- D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

Answer: A

Question #230

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.

- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Answer: B

Question #231

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

Which storage solution meets these requirements?

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

Question #232

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure environment on AWS in case the on-premises data center fails.

The company runs web servers that connect to external vendors. The data available on AWS and on premises must be uniform.

Which solution should a solutions architect recommend that has the LEAST amount of downtime?

- A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
- D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

Answer: A

Question #233

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Answer: B

Question #234

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Answer: D

Question #235

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.

What is the MOST cost-effective method to establish this type of connection?

- A. Implement a client VPN.
- B. Implement AWS Direct Connect.
- C. Implement a bastion host on Amazon EC2.
- D. Implement an AWS Site-to-Site VPN connection.

Answer: D

Question #236

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year.

The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

- A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
- B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
- C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
- D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

Answer: C

Question #237

A company runs a high performance computing (HPC) workload on AWS. The workload required low-latency network performance and high network throughput with tightly coupled node-to-node communication. The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.

What should a solutions architect propose to improve the performance of the workload?

- A. Choose a cluster placement group while launching Amazon EC2 instances.
- B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
- C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
- D. Choose the required capacity reservation while launching Amazon EC2 instances.

Answer: A

Question #238

A company uses a legacy on-premises analytics application that operates on gigabytes of .csv files and represents months of data. The legacy application cannot handle the growing size of .csv files. New .csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services. To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solutions architect recommend?

- A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company's on-premises storage and the company's S3 bucket.
- B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.
- C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.
- D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon EFS to the company's S3 bucket.

Answer: B

Question #239

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a

Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.

What should a solutions architect recommend?

- A. Set up a corporate Amazon S3 bucket and move all media and application files.
- B. Configure Amazon FSx for Windows File Server and move all the media and application files.
- C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
- D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

Answer: B

Reference:

<https://aws.amazon.com/fsx/windows/>

Question #240

A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the

VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances.

What should a solutions architect do to ensure these requirements are met?

- A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

- B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.
- C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

Answer: C

Question #241

A company is experiencing growth as demand for its product has increased. The company's existing purchasing application is slow when traffic spikes. The application is a monolithic three-tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier. A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes.

Which solution will meet these requirements?

- A. Vertically scale the application instance using a larger Amazon EC2 instance size.
- B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS.
- C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.
- D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

Answer: C

Question #242

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than

5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Answer: B

Question #243

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use of AWS Snowball.

What should a solutions architect recommend to accomplish this?

- A. Order a Snowball Edge device to copy the data from one Region to another Region.
- B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
- C. Use the aws s3 sync command to copy data from the source bucket to the destination bucket.
- D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

Answer: D

Question #244

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Answer: C

Question #245

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.

What should a solutions architect recommend?

- A. Use an Auto Scaling group with a cluster placement group.
- B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
- C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
- D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

Answer: A

Question #246

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Answer: D

Question #247

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available. The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.

What should a solutions architect recommend?

- A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
- B. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.
- C. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
- D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

Answer: B

Question #248

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not

able to delete objects in the bucket. The company follows least-privilege access rules.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "s3>ListBucket",  
                "s3>DeleteObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::bucket-name"  
            ],  
            "Effect": "Allow"  
        }  
    ]  
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

A.

```
"Action": [  
    "s3:*Object"  
,  
"Resource": [  
    "arn:aws:s3:::bucket-name/*"  
,  
"Effect": "Allow"
```

B.

```
"Action": [  
    "s3:*"  
,  
"Resource": [  
    "arn:aws:s3:::bucket-name/*"  
,  
"Effect": "Allow"
```

C.

```
"Action": [  
    "s3>DeleteObject"  
,  
"Resource": [  
    "arn:aws:s3:::bucket-name*"  
,  
"Effect": "Allow"
```

D.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

Answer: A

Question #249

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

Answer: C

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html

Question #250

A company wants to share forensic accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and requires its own copy of the database.

How should the company securely share the database with the auditor?

- A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.
- B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.
- C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.
- D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

Answer: A

Question #251

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

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

Answer: D

Question #252

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an

Amazon DynamoDB table. The metadata is used for searching and navigation.

The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Answer:B

Question #253

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Answer: B

Question #254

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

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

Answer: C

Reference:

<https://aws.amazon.com/blogs/database/best-storage-practices-for-running-production-workloads-on-hosted-databases-with-amazon-rds-or-amazon-ec2/>

Question #255

A solutions architect is designing a multi-Region disaster recovery solution for an application that will provide public API access. The application will use Amazon

EC2 instances with a userdata script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the

Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost?

- A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.

B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.

C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.

D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

Answer: D

Question #256

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBC snapshots are encrypted.

What should the solutions architect do to accomplish this?

- A. Enable EBS encryption by default for the AWS Region.
- B. Enable EBS encryption by default for the specific volumes.
- C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.
- D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#volume-account-off>

Question #257

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.

What should a solutions architect recommend to meet these requirements?

- A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
- B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
- C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
- D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Answer: AD

Question #258

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of

60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

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

Answer: A

Question #259

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront. The company has users in the United States, Canada, and Europe and wants to reduce costs.

What should a solutions architect recommend?

- A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.
- B. Implement CloudFront events with Lambda@Edge to run the website's data processing.
- C. Modify the CloudFront price class to include only the locations of the countries that are served.
- D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

Answer: C

Question #260

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

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

Answer: C

Question #261

A company is designing a website that uses an Amazon S3 bucket to store static images. The company wants all future requests to have faster response times while reducing both latency and cost.

Which service configuration should a solutions architect recommend?

- A. Deploy a NAT server in front of Amazon S3.
- B. Deploy Amazon CloudFront in front of Amazon S3.
- C. Deploy a Network Load Balancer in front of Amazon S3.
- D. Configure Auto Scaling to automatically adjust the capacity of the website.

Answer: B

Reference:

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

Question #262

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

Answer: AB

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/migrate-mysql-rds-dms/>

Question #263

A company needs to comply with a regulatory requirement that states all emails must be stored and archived externally for 7 years. An administrator has created compressed email files on premises and wants a managed service to transfer the files to AWS storage.

Which managed service should a solutions architect recommend?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon S3 Glacier
- C. AWS Backup
- D. AWS Storage Gateway

Answer: D

Reference:

<https://aws.amazon.com/storagegateway/faqs/>

<https://itexamcertified.com/>

Question #264

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named CompanyConfidential. The cloud engineer must be able to read from and write to an S3 bucket called AdminTools. Which IAM policy will meet these requirements?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": "arn:aws:s3:::AdminTools"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": [  
                "arn:aws:s3:::AdminTools",  
                "arn:aws:s3:::CompanyConfidential/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": "arn:aws:s3:::CompanyConfidential"  
        }  
    ]  
}
```

C.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*",  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

D.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential",  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::AdminTools/*"  
            ]  
        }  
    ]  
}
```

Answer: C

Question #265

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.

What should a solutions architect do to accomplish this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Answer: A

Reference:

Question #266

A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS.

Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.

The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.

Which solution meets these requirements?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
- B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

Answer: B

Question #267

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Choose two.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53.
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Answer: DE

Question #268

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.

What should a solutions architect do to minimize the anticipated server load?

- A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.
- B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
- C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
- D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

Answer: C

Question #269

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.

Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Answer:D

Question #270

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solutions architect recommend to provide a highly available and scalable solution?

- A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
- B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
- C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.
- D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

Answer: A

Question #271

Management has decided to deploy all AWS VPCs with IPv6 enabled. After some time, a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet.

What should the solutions architect do to fix this?

- A. Check to make sure that only IPv6 was used during the VPC creation.
- B. Create a new IPv4 subnet with a larger range, and then launch the instance.
- C. Create a new IPv6-only subnet with a large range, and then launch the instance.
- D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

Answer: C

Question #272

A company has a build server that is in an Auto Scaling group and often has multiple Linux instances running. The build server requires consistent and mountable shared NFS storage for jobs and configurations.

Which storage option should a solutions architect recommend?

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

Answer: A

Reference:

<https://aws.amazon.com/efs/>

Question #273

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a

NAT instance for internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

- A. Configure a NAT gateway to replace the NAT instances.
- B. Configure a gateway endpoint for traffic destined to Amazon S3.
- C. Configure an interface endpoint for traffic destined to Amazon S3.
- D. Configure Amazon CloudFront for the S3 bucket storing the images.

Answer:CB

Question #274

The financial application at a company stores monthly reports in an Amazon S3 bucket. The vice president of finance has mandated that all access to these reports be logged and that any modifications to the log files be detected.

Which actions can a solutions architect take to meet these requirements?

- A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled.
- B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled.
- C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.
- D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

Answer: C

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-cloudtrail-events.html>

Question #275

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Answer: D

Question #276

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company's account. All the needed policies have been created to grant appropriate access.

<https://itexamcertified.com/>

Which additional component will provide the vendor with the MOST secure access to the account?

- A. Create an IAM user.
- B. Implement a service control policy (SCP)
- C. Use a cross-account role with an external ID.
- D. Configure a single sign-on (SSO) identity provider.

Answer: C

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#data-from-iam

Question #277

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Answer: AD

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #278

A company has an ecommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS.

However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.

<https://itexamcertified.com/>

- C. Build a database cache using Amazon ElastiCache.
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Answer: C

Reference:

<https://aws.amazon.com/redis/>

Question #279

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices.

The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.
- B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

Answer: AD

Reference:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

Question #280

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users. During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Answer: C

Question #281

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Answer: C

Question #282

A company is backing up on-premises databases to local file server shares using the SMB protocol. The company requires immediate access to 1 week of backup files to meet recovery objectives. Recovery after a week is less likely to occur, and the company can tolerate a delay in accessing those older backup files.

What should a solutions architect do to meet these requirements with the LEAST operational effort?

- A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.
- B. Deploy an AWS Storage Gateway file gateway with sufficient storage to hold 1 week of backups. Point the backups to SMB shares from the file gateway.
- C. Deploy Amazon Elastic File System (Amazon EFS) to create a file system with exposed NFS shares with sufficient storage to hold all the desired backups.
- D. Continue to back up to the existing file shares. Deploy AWS Database Migration Service (AWS DMS) and define a copy task to copy backup files older than 1 week to Amazon S3, and delete the backup files from the local file store.

Answer: B

Question #283

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon

EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a period of time during surges. A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

Answer: D

Question #284

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solution architect needs to bring that data on premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.
- D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Answer:D

Question #285

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.

D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Answer: A

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html>

Question #286

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

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

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

Answer: B

Question #287

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be executed when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be executed when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Answer: D

Question #288

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Answer: B

Question #289

A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled. For compliance reasons, the older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.

What should the solutions architect recommend to meet these requirements at the LOWEST cost?

- A. Use S3 batch operations to replace object tags. Expire the objects based on the modified tags.
- B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.
- C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SQS) queue for further processing.
- D. Replicate older object versions to a new bucket. Use an S3 Lifecycle policy to expire the objects in the new bucket after 2 years.

Answer: B

Question #290

A company runs an application on an Amazon EC2 instance backed by Amazon Elastic Block Store (Amazon EBS). The instance needs to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application. However, the contents of the instance's memory must be preserved whenever the instance is unavailable.

What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.

D. Terminate the instance outside the application's availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Answer: B

Question #291

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from

0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Answer: C

Question #292

A company hosts historical weather records in Amazon S3. The records are downloaded from the company's website by a way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company's root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.

B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.

C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Answer: B

Question #293

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

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

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

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Answer: B

Question #294

A company is moving its on-premises applications to Amazon EC2 instances. However, as a result of fluctuating compute requirements, the EC2 instances must always be ready to use between 8 AM and 5 PM in specific Availability Zones.

Which EC2 instances should the company choose to run the applications?

- A. Scheduled Reserved Instances
- B. On-Demand Instances
- C. Spot Instances as part of a Spot Fleet
- D. EC2 instances in an Auto Scaling group

Answer: A

Question #295

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.

- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Answer: D

Question #296

A company is building an application on Amazon EC2 instances that generates temporary transactional data. The application requires access to data storage that can provide configurable and consistent IOPS.

What should a solutions architect recommend?

- A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
- B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
- C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.
- D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

Answer: C

Question #297

A solutions architect needs to design a resilient solution for Windows users' home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company's Active Directory.

Which storage solution meets these requirements?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Answer: B

Question #298

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Answer:A

Question #299

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting high request latency for users located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

How should a solutions architect accomplish this?

- A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
- C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Answer: B

Question #300

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users. The service is hosted in a VPC behind a

Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.

What should a solutions architect do to accomplish this goal?

- A. Create a peering VPC connection from each user's VPC to the software vendor's VPC.
- B. Deploy a transit VPC in the software vendor's AWS account. Create a VPN connection with each user account.
- C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.
- D. Deploy a transit VPC in the software vendor's AWS account. Create an AWS Direct Connect connection with each user account.

Answer: C

Question #301

A user wants to list the IAM role that is attached to their Amazon EC2 instance. The user has login access to the EC2 instance but does not have IAM permissions.

What should a solutions architect do to retrieve this information?

- A. Run the following EC2 command: curl http://169.254.169.254/latest/meta-data/iam/info
- B. Run the following EC2 command: curl http://169.254.169.254/latest/user-data/iam/info
- C. Run the following EC2 command: http://169.254.169.254/latest/dynamic/instance-identity/
- D. Run the following AWS CLI command: aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

Answer: A

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Question #302

A company has an application that is hosted on Amazon EC2 instances in two private subnets. A solutions architect must make the application available on the public internet with the least amount of administrative effort.

What should the solutions architect recommend?

- A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.
- D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two private subnets from the same Availability Zones as the public instances.

Answer:A

Question #303

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Answer: C

Question #304

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

Answer: A

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html>

Question #305

A company hosts its multi-tier public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon

RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes.

What should the solutions architect do to meet this requirement?

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

Answer: B

Question #306

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL. In the database layer several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Answer: D

Question #307

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.

- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Answer: D

Question #308

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

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

Answer: D

Question #309

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.

The following are the key requirements:

- ☞ The web servers must be accessible only to users on an SSL connection.
- ☞ The database should be accessible to the web layer, which is created in a public subnet only.

⇒ All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Select two.)

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0).
- B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
- C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.
- E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Answer: BD

Question #310

A company has an on-premises application that collects data and stores it to an on-premises NFS server. The company recently set up a 10 Gbps AWS Direct

Connect connection. The company is running out of storage capacity on premises. The company needs to migrate the application data from on premises to the

AWS Cloud while maintaining low-latency access to the data from the on-premises application.

What should a solutions architect do to meet these requirements?

- A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.
- C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

Answer: A

Question #311

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement and support the NFS protocol.

Which solution meets these requirements?

- A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
- B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the Instances and apply that to the additional instance.
- C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 Instances that need access to the data.
- D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Answer: A

Question #312

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability. The company wants to be able to deploy updates to its application even if nodes in one Availability Zone are not accessible.

The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to 100%.

Which configuration of tasks and Availability Zones meets these requirements?

- A. Deploy the application across two Availability Zones, with one task in each Availability Zone.
- B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
- C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
- D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

Answer: A

Question #313

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.

D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Answer: A

Question #314

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on

Amazon EC2 instances in different AWS Regions and a stateless UOP-based workload hosted on premises.

Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

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

Answer: AD

Question #315

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand

Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application

Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

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

Answer: A

Question #316

A company has an ecommerce application running in a single VPC. The application stack has a single web server and an Amazon RDS Multi-AZ DB instance.

The company launches new products twice a month. This increases website traffic by approximately 400% for a minimum of 72 hours. During product launches, users experience slow response times and frequent timeout errors in their browsers.

What should a solutions architect do to mitigate the slow response times and timeout errors while minimizing operational overhead?

- A. Increase the instance size of the web server.
- B. Add an Application Load Balancer and an additional web server.
- C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.
- D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

Answer: A

Question #317

A solutions architect is designing an architecture to run a third-party database server. The database software is memory intensive and has a CPU-based licensing model where the cost increases with the number of vCPU cores within the operating system. The solutions architect must select an Amazon EC2 instance with sufficient memory to run the database software, but the selected instance has a large number of vCPUs. The solutions architect must ensure that the vCPUs will not be underutilized and must minimize costs.

Which solution meets these requirements?

- A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.
- B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.
- C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.
- D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

Answer: A

Question #318

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Answer:ab

Question #319

A company is creating a web application that will store a large number of images in Amazon S3. The images will be accessed by users over variable periods of time. The company wants to:

- Retain all the images
- Incur no cost for retrieval.
- Have minimal management overhead.
- Have the images available with no impact on retrieval time.

Which solution meets these requirements?

- A. Implement S3 Intelligent-Tiering
- B. Implement S3 storage class analysis
- C. Implement an S3 Lifecycle policy to move data to S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Implement an S3 Lifecycle policy to move data to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: A

Question #320

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.

- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Answer:D

Question #321

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order, two microservices should handle the event simultaneously. The Email microservice will send a confirmation email, and the OrderProcessing microservice will start the order delivery process. If a customer cancels an order, the OrderCancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

- A. Create a single SQS queue and publish order events to it. The Email OrderProcessing and Order Cancellation microservices can then consume messages of the queue.
- B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email OrderProcessing and Order Cancellation microservices to its own topic.
- C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email OrderProcessing and Order Cancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.
- D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and Order Cancellation microservices.

Answer: C

Question #322

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL

Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon EBS General Purpose SSD (gp2) volume. The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a Magnetic volume.

- B. Increase the number of IOPS on the gp2 volume.
- C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
- D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Answer: C

Question #323

A company has an application that uses Amazon Elastic File System (Amazon EFS) to store data. The files are 1 GB in size or larger and are accessed often only for the first few days after creation. The application data is shared across a cluster of Linux servers. The company wants to reduce storage costs for the application.

What should a solutions architect do to meet these requirements?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon EFS and store them locally on each Amazon EC2 instance.
- C. Configure a Lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
- D. Move the files to Amazon S3 with S3 lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

Answer: C

Question #324

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solution architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Answer: A

Question #325

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

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

Answer: A

Question #326

A company wants to migrate its web application to AWS. The legacy web application consists of a web tier, an application tier, and a MySQL database. The re-architected application must consist of technologies that do not require the administration team to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Choose two.)

- A. Amazon Aurora Serverless
- B. Amazon EC2 Spot Instances
- C. Amazon Elasticsearch Service (Amazon ES)
- D. Amazon RDS for MySQL
- E. AWS Fargate

Answer: DE

Question #327

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier two application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).

<https://itexamcertified.com/>

D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Answer: B

Question #328

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.
- D. Increase the Provisioned IOPS on the Aurora instance.

Answer: D

Question #329

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

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

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Answer: DB

<https://aws.amazon.com/storagegateway/file/>

Question #330

A solution architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

<https://itexamcertified.com/>

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Amazon EC2 instances in private subnets Configure. Configure a public Application Load Balancer with multiple redundant Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Answer: B

Question #331

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region it runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in- memory cache for DynamoDB hosting the application data.

Answer: A

Question #332

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in

Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

- A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
- D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Answer: C

Question #333

A development team stores its Amazon RDS MySQL DB instance user name and password credentials in a configuration file. The configuration file is stored as plaintext on the root device volume of the team's Amazon EC2 instance. When the team's application needs to reach the database, it reads the file and loads the credentials into the code. The team has modified the permissions of the configuration file so that only the application can read its content. A solution architect must design a more secure solution.

What should the solutions architect do to meet this requirement?

- A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.
- B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.
- C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.
- D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

Answer: B

Question #334

A company wants a storage option that enables its data science team to analyze its data on premises and in the AWS Cloud. The team needs to be able to run statistical analyses by using the data on premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones.

What should a solutions architect do to meet these requirements?

- A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
- B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
- C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

Answer: D

Question #335

A company wants to improve the availability and performance of its stateless UDP-based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions.

What should a solutions architect recommend to accomplish this?

- A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
- B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.
- C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
- D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

Answer: D

Question #336

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each

HPC workflow runs on hundreds of AmazonEC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Answer: A

Question #337

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead from aging and scaling the database must be minimized.

Which database solution should the solutions architect recommend?

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

D. Amazon Redshift

Answer: B

Question #338

A company is working with an external vendor that requires write access to the company's Amazon Simple Queue Service (Amazon SQS) queue. The vendor has its own AWS account.

What should a solutions architect do to implement least privilege access?

- A. Update the permission policy on the SQS queue to give write access to the vendor's AWS account.
- B. Create an IAM user with write access to the SQS queue and share the credentials for the IAM user.
- C. Update AWS Resource Access Manager to provide write access to the SQS queue from the vendor's AWS account.
- D. Create a cross-account role with access to all SQS queues and use the vendor's AWS account in the trust document for the role.

Answer: D

Question #339

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.

The tracking will need to read as fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of packages might be tracked on other days. Tracking will need to be searchable by tracking ID, customer ID, and order ID. Orders older than 1 month no longer need to be tracked.

What should a solution architect recommend to accomplish this with minimal cost of ownership?

- A. Use Amazon DynamoDB with Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
- B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.

- C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
- D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

Answer: B

Question #340

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

Answer: C

Question #341

A company needs to store data in Amazon S3. A compliance requirement states that when any changes are made to objects the previous state of the object with any changes must be preserved. Additionally, files older than 5 years should not be accessed but need to be archived for auditing.

What should a solutions architect recommend that is MOST cost-effective?

- A. Enable object-level versioning and S3 Object Lock in governance mode
- B. Enable object-level versioning and S3 Object Lock in compliance mode

- C. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive
- D. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: C

Question #342

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Answer: DE

Question #343

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings in the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur they will happen very quickly.

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.

- B. Create a DynamoDB table with a global secondary index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Answer: A

Question #344

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Answer: D

Question #345

A company is preparing to deploy a new serverless workload. A solutions architect needs to configure permissions for invoking an AWS Lambda function. The function will be triggered by an Amazon EventBridge (Amazon CloudWatch Events) rule. Permissions should be configured using the principle of least privilege.

Which solution will meet these requirements?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.

- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Answer: C

Question #346

A company is building its web application using containers on AWS. The company requires three instances of the web application to run at all times. The application must be able to scale to meet increases in demand. Management is extremely sensitive to cost but agrees that the application should be highly available.

What should a solutions architect recommend?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

Answer: A

Question #347

A company is Re-architecting a strongly coupled application to be loosely coupled. Previously the application used a request/response pattern to communicate between tiers. The company plans to use Amazon Simple Queue Service (Amazon SQS) to achieve decoupling requirements. The initial design contains one queue for requests and one for responses. However, this approach is not processing all the messages as the application scales.

What should a solutions architect do to resolve this issue?

- A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.
- B. Configure a FIFO queue, and use the message deduplication ID and message group ID.
- C. Create a temporary queue, with the Temporary Queue Client to receive each response message.
- D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

Answer: C

Question #348

A company is launching an ecommerce website on AWS. This website is built with a three-tier architecture that includes a MySQL database in a Multi-AZ deployment of Amazon Aurora MySQL. The website application must be highly available and will initially be launched in an AWS Region with three Availability

Zones The application produces a metric that describes the load the application experiences.

Which solution meets these requirements?

- A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling
- B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
- C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.
- D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

Answer: B

Question #349

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

Answer: A

Question #350

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice

B.

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

- A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Answer: B

Question #351

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3. Which solution meets these requirements and is MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Answer: B

Question #352

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

Which solution meets these requirements?

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

Answer: A

Question #353

A company has multiple applications that use Amazon RDS for MySQL as its database. The company recently discovered that a new custom reporting application has increased the number of Queries on the database. This is slowing down performance.

How should a solutions architect resolve this issue with the LEAST amount of application changes?

- A. Add a secondary DB instance using Multi-AZ.
- B. Set up a read replica and Multi-AZ on Amazon RDS.
- C. Set up a standby replica and Multi-AZ on Amazon RDS.
- D. Use caching on Amazon RDS to improve the overall performance.

Answer: D

Question #354

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that security and compliance standards are being followed throughout the development process.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.
- B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.
- C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

Answer: C

Question #355

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month.

Which analytics strategy is MOST cost-effective for the company to use?

- A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.

B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.

C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.

D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

Answer: B

Question #356

A company wants to move its on-premises network, attached storage (NAS) to AWS. The company wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time.

Which solution meets these requirements and is MOST cost-effective?

A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.

B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.

C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.

D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

Answer: D

Question #357

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.

How should the company write its application to handle these database requests?

- A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
- B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Answer: A

Question #358

A company that recently started using AWS establishes a Site-to-Site VPN between its on-premises datacenter and AWS. The company's security mandate states that traffic originating from on premises should stay within the company's private IP space when communicating with an Amazon Elastic Container Service

(Amazon ECS) cluster that is hosting a sample web application.

Which solution meets this requirement?

- A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.
- B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.
- C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.
- D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

Answer: C

Question #359

A solutions architect must analyze and update a company's existing IAM policies prior to deploying a new workload. The solutions architect created the following policy:

What is the net effect of this policy?

- A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.
- C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

Answer: D

Question #360

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a

PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Answer: CD

Question #361

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Answer: D

Question #362

A company is using Amazon DynamoDB with provisioned throughput for the database tier of its ecommerce website. During flash sales, customers experience periods of time when the database cannot handle the high number of transactions taking place. This causes the company to lose transactions. During normal periods, the database performs appropriately.

Which solution solves the performance problem the company faces?

- A. Switch DynamoDB to on-demand mode during flash sales.
- B. Implement DynamoDB Accelerator for fast in memory performance.
- C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.
- D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

Answer: A

Question #363

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B

Question #364

A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.

What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

- A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
- B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

Answer: A

Question #365

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue

Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

- A. Create an instance profile that provides the other company access to the SQS queue.
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Answer: C

Question #366

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and a paid tier. Users in the paid tier will have their videos converted first and then the tree tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

- A. One FIFO queue for the paid tier and one standard queue for the free tier.
- B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

Answer: D

Question #367

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company's AWS accounts.

Which AWS service can the administrator use to protect the company against attacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

Answer: C

Question #368

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company's security policy states that any external service cannot initiate a connection to the EC2 instances. What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table.
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Answer: D

Question #369

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon

Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

Answer: A

Question #370

A company wants to host its web application on AWS using multiple Amazon EC2 instances across different AWS Regions. Since the application content will be specific to each geographic region, the client requests need to be routed to the server that hosts the content for that clients Region.

What should a solutions architect do to accomplish this?

- A. Configure Amazon Route 53 with a latency routing policy.
- B. Configure Amazon Route 53 with a weighted routing policy.
- C. Configure Amazon Route 53 with a geolocation routing policy.
- D. Configure Amazon Route 53 with a multivalue answer routing policy

Answer: C

Question #371

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability. Which solution meets these requirements?

- A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.

- B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
- C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
- D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Answer: A

Question #372

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs.

What should a solutions architect recommend to accomplish this?

- A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
- B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
- C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.
- D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

Answer: C

Question #373

A company is building a payment application that must be highly available even during regional service disruptions. A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions. The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports. The development team also needs to use SQL.

Which data storage solution meets these requirements?

- A. Amazon Aurora Global Database

- B. Amazon DynamoDB global tables
- C. Amazon S3 with cross-Region replication and Amazon Athena
- D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

Answer: C

Question #374

A company stores call recordings on a monthly basis. Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year.

Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost.

Which solution is MOST cost-effective?

- A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier Query S3 Glacier tags and retrieve the files from S3 Glacier.
- B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
- C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

Answer: B

Question #375

A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

- A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.
- B. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.
- C. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.
- D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

Answer: D

Question #376

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

- A. Amazon S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

Answer: D

Question #377

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an

Elastic Load Balancer (ELB). A third party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against largescale DDoS attacks.

Which solution meets these requirements?

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

Answer: D

Question #378

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Answer: C

Question #379

A company is running a multi-tier web application on AWS. The application runs its database tier on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region. A database administrator who regularly monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica and causing increased read latency of the application.

What should a solutions architect do to improve read scalability?

- A. Reboot the Aurora DB cluster.
- B. Create a cross-Region read replica
- C. Increase the instance class of the read replica.
- D. Configure Aurora Auto Scaling for the read replica.

Answer: D

Question #380

A company's order fulfillment service uses a MySQL database. The database needs to support a large number of concurrent queries and transactions. Developers are spending time patching and tuning the database. This is causing delays in releasing new product features.

The company wants to use cloud-based services to help address this new challenge. The solution must allow the developers to migrate the database with little or no code changes and must optimize performance.

Which service should a solutions architect use to meet these requirements?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon ElastiCache
- D. MySQL on Amazon EC2

Answer: A

Question #381

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company want to run complex transformation before transferring the data.

Which AWS service should a solutions architect recommend for this migration?

- A. AWS Snowball
- B. AWS Snowmobile
- C. AWS Snowball Edge Storage Optimize
- D. AWS Snowball Edge Compute Optimize

Answer: D

Question #382

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Answer: A

Question #383

A company is selling up an application to use an Amazon RDS MySQL DB instance. The database must be architected for high availability across Availability Zones and AWS Regions with minimal downtime.

<https://itexamcertified.com/>

How should a solutions architect meet this requirement?

- A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.
- B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.
- C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.
- D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

Answer: C

Question #384

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multi-value routing policy
- D. Geolocation routing policy

Answer: C

Question #385

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data needs to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

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

Answer: D

Question #386

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy for data at rest in Amazon S3. The company's security policy states:

- ⇒ Keys must be rotated every 90 days.
- ⇒ Strict separation of duties between key users and key administrators must be implemented.
- ⇒ Auditing key usage must be possible.

What should the solutions architect recommend?

- A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
- C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
- D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

Answer: A

Question #387

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate

accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.

Which storage solution is MOST cost-effective?

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

Answer: C

Question #388

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in the same Region.

Answer: D

Question #389

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in older.

What should a solutions architect recommend to decouple the system?

- A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.
- B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.
- D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

Answer: C

Question #390

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy.

Which solution meets these requirements?

- A. Replace the NAT gateway with a NAT instance.
- B. Replace the NAT gateway with an internet gateway.
- C. Replace the NAT gateway with a gateway VPC endpoint.
- D. Replace the NAT gateway with an AWS Direct Connect connection.

Answer: C

Question #391

A company hosts a website on premises and wants to migrate it to the AWS Cloud. The website exposes a single hostname to the internet but it routes its functions to different on-premises server groups based on the path of the URL. The server groups are scaled independently depending on the needs of the functions they support. The company has an AWS Direct Connect connection configured to its on-premises network.

What should a solutions architect do to provide path-based routing to send the traffic to the correct group of servers?

- A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.
- B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.
- C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.
- D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer for the group of servers supporting that path.

Answer: C

Question #392

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage auto scaling in RDS.
- B. Increase the RDS database instance size.
- C. Change the RDS database instance storage type to Provisioned IOPS.
- D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

Answer: A

Question #393

An ecommerce website is deploying its web application as Amazon Elastic Container Service (Amazon ECS) container instances behind an Application Load

Balancer (ALB). During periods of high activity, the website slows down and availability is reduced. A solutions architect uses Amazon CloudWatch alarms to receive notifications whenever there is an availability issue so they can scale out resources. Company management wants a solution that automatically responds to such events.

Which solution meets these requirements?

- A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Setup AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Answer: D

Question #394

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results. A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.
- C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.
- D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on- demand capacity scaling enabled.

Answer: B

Question #395

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

- A. Modify the shipping application to write to a local database.
- B. Modify the application APIs to run serverless using AWS Lambda
- C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
- D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

Answer: D

Question #396

A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to

Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB.
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

Answer: C

Question #397

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
- D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Answer: C

Question #398

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform

SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.

B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.

C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.

D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Answer: D

Question #399

A web application must persist order data to Amazon S3 to support near-real time processing. A solutions architect needs to create an architecture that is both scalable and fault tolerant.

Which solutions meet these requirements? (Choose two.)

A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Answer: AB

Question #400

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions. To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.

What should a solutions architect do to accomplish this?

- A. Create a NAT gateway and update the route table of the EC2 instances' subnet.
- B. Create a VPC endpoint and update the route table of the EC2 instances' subnet.
- C. Create a VPN connection and update the route table of the EC2 instances' subnet.
- D. Create a VPC peering connection and update the route table of the EC2 instances' subnet.

Answer: D

Question #401

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.

Which application change should a solutions architect recommend to resolve these issues?

- A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
- B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
- C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
- D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

Answer: C

Question #402

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Answer: D

Question #403

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The database cannot be migrated to a different engine because SQL Server features are used in the application's NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

- A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.
- B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
- C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

Answer: B

Question #404

A company has an application running on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3. To reduce costs, the company wants to configure its AWS resources in a cost-effective manner.

How should the company accomplish this?

- A. Deploy a NAT gateway to access the S3 buckets.
- B. Deploy AWS Storage Gateway to access the S3 buckets.
- C. Deploy an S3 gateway endpoint to access the S3 buckets.
- D. Deploy an S3 interface endpoint to access the S3 buckets.

Answer: C

Question #405

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a fleet of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only. No data can be lost during the deployment.

What should a solutions architect recommend?

- A. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
- B. Use Amazon Kinesis Data Streams to capture the data from the websites, Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
- D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Answer: B

Question #406

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long

periods of time when the EC2 instances were not being used. A solutions architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

- A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
- B. Build the application to use Amazon Lightsail with On-Demand Instances.
- C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.
- D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

Answer: D

Question #407

A company is using Site-to-Site VPN connections for secure connectivity to its AWS Cloud resources from on premises. Due to an increase in traffic across the

VPN connections to the Amazon EC2 instances, users are experiencing slower VPN connectivity.

Which solution will improve the VPN throughput?

- A. Implement multiple customer gateways for the same network to scale the throughput.
- B. Use a transit gateway with equal cost multipath routing and add additional VPN tunnels.
- C. Configure a virtual private gateway with equal cost multipath routing and multiple channels.
- D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

Answer: A

Question #408

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots replication and sub-millisecond response times.

What should the solutions architect recommend to solve these issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Answer: C

Question #409

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly. Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.
- B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Answer: C

Question #410

A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these

Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy.
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

Answer: A

Question #411

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS

Key Management Service Customer Master Keys (AWS KMS CMKs). A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy.
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Answer: BE

Question #412

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. To meet the migration date, minimal changes can be made.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web server.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
- D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

Answer: C

Question #413

A company that operates a web application on premises is preparing to launch a newer version of the application on AWS. The company needs to route requests to either the AWS-hosted or the on-premises-hosted application based on the URL query string. The on-premises application is not available from the internet, and a VPN connection is established between Amazon VPC and the company's data center. The company wants to use an Application Load Balancer (ALB) for this launch.

Which solution meets these requirements?

- A. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to each target group of each ALB. Route with Amazon Route 53 based on the URL query string.
- B. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to the target group of each ALB. Create a software router on an EC2 instance based on the URL query string.
- C. Use one ALB with two target groups: one for the AWS resource and one for on premises. Add hosts to each target group of the ALB. Configure listener rules based on the URL query string.
- D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on premises. Add hosts to each Auto Scaling group. Route with Amazon Route 53 based on the URL query string.

Answer: A

Question #414

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.

Which solution meets these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
- B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
- C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Answer: C

Question #415

A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

- A. Use AWS Snowball Edge devices to process and store the images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.
- D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Answer: B

Question #416

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application, data layer that uses Oracle-specific PSQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and RDS instance to run out of

storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Answer: AC

Question #417

An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.

How should the permissions for the team be configured so they also adhere to the concept of least privilege?

- A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.
- B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group.
- C. Create an execution role for the Lambda functions. Attach a managed policy that has permission boundaries specific to these Lambda functions.
- D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions. Allow the engineering team to assume this role.

Answer: A

Question #418

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains over 10 million rows. The database has 2 TB of General Purpose SSD (gp2) storage. There are millions of updates against this data every day through the company's website. The company has noticed some operations are taking 10 seconds or longer and has determined that the database storage performance is the bottleneck.

Which solution addresses the performance issue?

- A. Change the storage type to Provisioned IOPS SSD (io1).
- B. Change the instance to a memory-optimized instance class.
- C. Change the instance to a burstable performance DB instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Answer: A

Question #419

A company has an Amazon S3 bucket that contains mission-critical data. The company wants to ensure this data is protected from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: AB

Reference:

<https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-LNMKnp7BP01IYVSlee8/Final%20practice%20exam>

Question #420

A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.

The application development team does not have time to make the necessary code modifications to move the application to AWS.

Which service should a solutions architect recommend to allow the application to copy files to AWS?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Windows File Server
- C. AWS Snowball
- D. AWS Storage Gateway

Answer: B

Reference:

<https://aws.amazon.com/blogs/storage/accessing-smb-file-shares-remotely-with-amazon-fsx-for-windows-file-server/>

Question #421

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (Choose two.)

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- B. Create a bucket policy to make the objects in the S3 bucket public.
- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Answer: AC

Question #422

A solutions architect plans to convert a company's monolithic web application into a multi-tier application. The company wants to avoid managing its own infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application's API.

Which solution meets these requirements?

- A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
- B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
- C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
- D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

Answer: A

Question #423

A team has an application that detects new objects being uploaded into an Amazon S3 bucket. The uploads trigger AWS Lambda function to write object metadata into an Amazon DynamoDB table and an Amazon RDS for PostgreSQL database.

Which action should the team take to ensure high availability?

- A. Enable Cross-Region Replication in the S3 bucket.
- B. Create a Lambda function for each Availability Zone the application is deployed in.
- C. Enable Multi-AZ on the RDS for PostgreSQL database.
- D. Create a DynamoDB stream for the DynamoDB table.

Answer: C

Question #424

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migration?

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

Answer: C

Question #425

An application calls a service run by a vendor. The vendor charges based on the number of calls. The finance department needs to know the number of calls that are made to the service to validate the billing statements.

How can a solutions architect design a system to durably store the number of calls without requiring changes to the application?

- A. Call the service through an internet gateway.
- B. Decouple the application from the service with an Amazon Simple Queue Service (Amazon SQS) queue.
- C. Publish a custom Amazon CloudWatch metric that counts calls to the service.
- D. Call the service through a VPC peering connection.

Answer: C

There are 2 main types of monitoring you can do on AWS EC2 Instances as follows:

Basic Monitoring for Amazon EC2 instances: Seven pre-selected metrics at five-minute frequency and three status check metrics at one-minute frequency, for no additional charge.

Detailed Monitoring for Amazon EC2 instances: All metrics available to Basic Monitoring at one-minute frequency, for an additional charge. Instances with Detailed

Monitoring enabled allows data aggregation by Amazon EC2 AMI ID and instance type.

Reference:

<https://datanextsolutions.com/blog/how-to-collect-custom-metrics-from-aws-ec2-instances/>

Question #426

A company wants to reduce its Amazon S3 storage costs in its production environment without impacting durability or performance of the stored objects.

What is the FIRST step the company should take to meet these objectives?

- A. Enable Amazon Macie on the business-critical S3 buckets to classify the sensitivity of the objects.
- B. Enable S3 analytics to identify S3 buckets that are candidates for transitioning to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Enable versioning on all business-critical S3 buckets.
- D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

Answer: D

Question #427

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

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

D. Amazon S3

Answer: C

Reference:

<https://www.missioncloud.com/blog/resource-amazon-ebs-vs-efs-vs-s3-picking-the-best-aws-storage-option-for-your-business>

Question #428

A company hosts multiple production applications. One of the applications consists of resources from Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple

Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) across multiple AWS Regions. All company resources are tagged with a tag name of `application` and a value that corresponds to each application. A solutions architect must provide the quickest solution for identifying all of the tagged components.

Which solution meets these requirements?

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

Answer: D

Question #429

A development team is deploying a new product on AWS and is using AWS Lambda as part of the deployment. The team allocates 512 MB of memory for one of the Lambda functions. With this memory allocation, the function is completed in 2 minutes. The function runs millions of times monthly, and the development team is concerned about cost. The team conducts tests to see how different Lambda memory allocations affect the cost of the function.

Which steps will reduce the Lambda costs for the product? (Choose two.)

- A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.

- B. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 90 seconds.
- C. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 4 minutes.
- D. Increase the memory allocation for this Lambda function to 2,048 MB if this change causes the execution time of each function to be less than 1 minute.
- E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

Answer: AE

Question #430

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon

EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

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

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Answer: AC

Question # 431

A gaming company is using Amazon DynamoDB to run a high-score leaderboard and record the game progress for users. The company is launching a new game that is expected to be active for years. The database activity at launch cannot be predicted; but it is expected to stabilize after 4 weeks. Currently, the company is using on-demand capacity mode for processing reads and writes on all DynamoDB tables. What is the MOST cost-effective way for the company to control the DynamoDB capacity during the new game launch?

- A. Use on-demand mode and purchase DynamoDB reserved capacity for the first 4 weeks of the game launch
- B. Use provisioned capacity mode, and purchase DynamoDB reserved capacity for the first 4 weeks of the game launch
- C. Use on-demand mode for the game launch, switch to provisioned capacity mode after 4 weeks and then purchase DynamoDB reserved capacity
- D. Use provisioned capacity mode for the game launch, switch back to on-demand mode after 4 weeks, and then purchase DynamoDB reserved capacity

Answer: C

Question #432

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

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

Answer: D

Question #433

A company has an application that uses overnight digital images of products on store shelves to analyze inventory data. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) and obtains the images from an Amazon S3 bucket for its metadata to be processed by worker nodes for analysis. A solutions architect needs to ensure that every image is processed by the worker nodes.

What should the solutions architect do to meet this requirement in the MOST cost-efficient way?

- A. Send the image metadata from the application directly to a second ALB for the worker nodes that use an Auto Scaling group of EC2 Spot Instances as the target group.
- B. Process the image metadata by sending it directly to EC2 Reserved Instances in an Auto Scaling group. With a dynamic scaling policy, use an Amazon CloudWatch metric for average CPU utilization of the Auto Scaling group as soon as the front-end application obtains the images.

C. Write messages to Amazon Simple Queue Service (Amazon SQS) when the front-end application obtains an image. Process the images with EC2 On-Demand instances in an Auto Scaling group with instance scale-in protection and a fixed number of instances with periodic health checks.

D. Write messages to Amazon Simple Queue Service (Amazon SQS) when the application obtains an image. Process the images with EC2 Spot Instances in an Auto Scaling group with instance scale-in protection and a dynamic scaling policy using a custom Amazon CloudWatch metric for the current number of messages in the queue.

Correct Answer: D

Question #434

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing.

Which solution will meet these requirements?

- A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
- B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
- C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
- D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Correct Answer: C

Reference:

Question #435

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on-premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.

B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.

C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Correct Answer: A

Question #436

A company manages its own Amazon EC2 instances that run MySQL databases. The company is manually managing replication and scaling as demand increases or decreases. The company needs a new solution that simplifies the process of adding or removing compute capacity to or from its database tier as needed. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Correct Answer: A

Reference:

<https://aws-quickstart.s3.amazonaws.com/quickstart-drupal/doc/drupal-on-the-aws-cloud.pdf>

(p.6)

Question #437

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure.

Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

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

Correct Answer: A

Question #438

A company has two AWS accounts: Production and Development. There are code changes ready in the Development account to push to the Production account.

In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers might need access to perform testing as well.

What should a solutions architect recommend?

- A. Create two policy documents using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Give one IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account with the trust policy that specifies the Development account. Allow developers to assume the role.
- D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account. Add developers to the group.

Correct Answer: C

Question #439

A company is using an Amazon S3 bucket to store data uploaded by different departments from multiple locations. During an AWS Well-Architected review, the financial manager notices that 10 TB of S3 Standard storage data has been

charged each month. However, in the AWS Management Console for Amazon S3, using the command to select all files and folders shows a total size of 5 TB.

What are the possible causes for this difference? (Choose two.)

- A. Some files are stored with deduplication.
- B. The S3 bucket has versioning enabled.
- C. There are incomplete S3 multipart uploads.
- D. The S3 bucket has AWS Key Management Service (AWS KMS) enabled.
- E. The S3 bucket has Intelligent-Tiering enabled.

Correct Answer: BC

Question #440

A user owns a MySQL database that is accessed by various clients who expect, at most, 100 ms latency on requests. Once a record is stored in the database, it is rarely changed. Clients only access one record at a time.

Database access has been increasing exponentially due to increased client demand. The resultant load will soon exceed the capacity of the most expensive hardware available for purchase. The user wants to migrate to AWS, and is willing to change database systems.

Which service would alleviate the database load issue and offer virtually unlimited scalability for the future?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. AWS Data Pipeline

Correct Answer: B

Reference:

<https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/>

Question #441

A company designs a mobile app for its customers to upload photos to a website. The app needs a secure login with multi-factor authentication (MFA). The company wants to limit the initial build time and the maintenance of the solution.

Which solution should a solutions architect recommend to meet these requirements?

- A. Use Amazon Cognito Identity with SMS-based MFA.

- B. Edit IAM policies to require MFA for all users.
- C. Federate IAM against the corporate Active Directory that requires MFA.
- D. Use Amazon API Gateway and require server-side encryption (SSE) for photos.

Correct Answer: A

Reference:

<https://aws.amazon.com/cognito/>

442.

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Placement groups

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Depending on the type of workload.

Cluster – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Reference: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

443.

QUESTION: 443

A client reports that they want see an audit log of any changes made to AWS resources in their account.

What can the client do to achieve this?

- A. Set up Amazon CloudWatch monitors on services they own
- B. Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket
- C. Use Amazon CloudWatch Events to parse logs
- D. Use AWS OpsWorks to manage their resources

Answer: B

Explanation:

A CloudTrail trail can be created which delivers log files to an Amazon S3

QUESTION: 444

An application running in a private subnet accesses an Amazon DynamoDB table. There is a security requirement that the data never leave the AWS network.

How should this requirement be met?

- A. Configure a network ACL on DynamoDB to limit traffic to the private subnet
- B. Enable DynamoDB encryption at rest using an AWS KMS key
- C. Add a NAT gateway and configure the route table on the private subnet
- D. Create a VPC endpoint for DynamoDB and configure the endpoint policy

Answer: D

Explanation:

Hint: Private Subnet = VPC Endpoint

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

QUESTION: 445

A three-tier application is being created to host small news articles. The application is expected to serve millions of users. When breaking news occurs, the site must handle very large spikes in traffic without significantly impacting database performance.

Which design meets these requirements while minimizing costs?

- A. Use Auto Scaling groups to increase the number of Amazon EC2 instances delivering the web application
- B. Use Auto Scaling groups to increase the size of the Amazon RDS instances delivering the database
- C. Use Amazon DynamoDB strongly consistent reads to adjust for the increase in traffic
- D. Use Amazon DynamoDB Accelerator (DAX) to cache read operations to the database

Answer: D

Explanation:

DAX has in memory cache. If breaking news happens, majority of the users searching will look for the exact same thing. That being said, requests will query the Memory Cache first and will not need to fetch the data from the DB directly.

QUESTION: 446

During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS.

What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?

- A. Create an import package of the application code for upload to AWS Lambda, and include a function to create another Lambda function to migrate data into an Amazon RDS database
- B. Create an image of the user's desktop, migrate it to Amazon EC2 using VM Import, and place the EC2 instance in an Auto Scaling group
- C. Pre-stage new Amazon EC2 instances running the application code on AWS behind an Application Load Balancer and an Amazon RDS Multi-AZ DB instance
- D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance. Migrate the application code to AWS Elastic Beanstalk

Answer: D

QUESTION: 447

A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the first 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the first 120 days, accessing these files should never take more than a few seconds.

Which lifecycle policy should be used for the S3 objects to minimize costs based on the access pattern?

- A. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage for the first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after

that.

- B. Use Amazon S3 Standard storage for the first 30 days. Then move the files to Amazon S3 Standard- Infrequent Access (S3 Standard-IA) for the next 90 days. Allow the data to expire after that.
- C. Use Amazon S3 Standard storage for first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.
- D. Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the first 30 days. After that, move the data to the GLACIER storage class, where it will be deleted automatically.

QUESTION: 448

An application generates audit logs of operational activities. Compliance requirements mandate that the application retain the logs for 5 years.

How can these requirements be met?

- A. Save the logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the bucket.
- B. Save the logs in an Amazon EFS volume and use Network File System version 4 (NFSv4) locking with the volume.
- C. Save the logs in an Amazon Glacier vault and use the Vault Lock feature.
- D. Save the logs in an Amazon EBS volume and take monthly snapshots.

Answer: C

Explanation:

Amazon Glacier, which enables long-term storage of mission-critical data, has added Vault Lock. This new feature allows you to lock your vault with a variety of compliance controls that are designed to support such long-term records retention.

QUESTION: 449

A Solutions Architect is creating an application running in an Amazon VPC that needs to access AWS Systems Manager Parameter Store. Network security rules prohibit any route table entry with a 0.0.0.0/0 destination.

What infrastructure addition will allow access to the AWS service while meeting the requirements?

- A. VPC peering
- B. NAT instance
- C. NAT gateway
- D. AWS PrivateLink

Answer: D

Explanation:

To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint. Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.

CORRECT: "Use AWS PrivateLink" is the correct answer.

INCORRECT: "Use an Internet Gateway" is incorrect. Internet Gateways are used by instances in public subnets to access the Internet and this is less secure than an VPC endpoint.

INCORRECT: "Use a proxy instance" is incorrect. A proxy instance will also use the public Internet and so is less secure than a VPC endpoint.

INCORRECT: "Use a NAT gateway" is incorrect. A NAT Gateway is used by instances in private subnets to access the Internet and this is less secure than an VPC endpoint.

References:

<https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html>

QUESTION: 450

A company is implementing a data lake solution on Amazon S3. Its security policy mandates that the data stored in Amazon S3 should be encrypted at rest.

Which options can achieve this? (Select TWO.)

- A. Use S3 server-side encryption with an Amazon EC2 key pair.
- B. Use S3 server-side encryption with customer-provided keys (SSE-C).
- C. Use S3 bucket policies to restrict access to the data at rest.
- D. Use client-side encryption before ingesting the data to Amazon S3 using encryption keys.
- E. Use SSL to encrypt the data while in transit to Amazon S3.

Answer: BD

QUESTION:451

You have set up an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?

- A. 11 minutes
- B. 7 minutes

- C. 10 minutes
- D. 14 minutes

Answer: A

Explanation:

If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.

Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION: 452

In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

- A. A cluster
- B. A container instance
- C. A container
- D. A task definition

Answer: A

Explanation:

Amazon ECS contains the following components:

A Cluster is a logical grouping of container instances that you can place tasks on. A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster.

A Task definition is a description of an application that contains one or more container definitions. A Scheduler is the method used for placing tasks on container instances. A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.

A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that was created as part of a task.

Reference: <http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html>

QUESTION: 453

In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

- A. Because most reachability issues are resolved by automated processes in less than 20 minutes
- B. Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine

- maintenance
- C. Because all EC2 instances are unreachable for 20 minutes when first launched
 - D. Because of all the reasons listed here

Answer: A

Explanation:

An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support.

Reference: <https://aws.amazon.com/premiumsupport/faqs/>

QUESTION: 454

Can a user get a notification of each instance start / terminate configured with Auto Scaling?

- A. Yes, if configured with the Launch Config
- B. Yes, always
- C. Yes, if configured with the Auto Scaling group
- D. No

Answer: C

Explanation:

The user can get notifications using SNS if he has configured the notifications while creating the Auto Scaling group.

Reference:

<http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html>

QUESTION: 455

Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

- A. snapshots
- B. images
- C. instance backups
- D. mirrors

Answer: A

Explanation:

Amazon allows you to make backups of the data stored in your EBS volumes through snapshots that can later be used to create a new EBS volume.

Reference: <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html>

QUESTION: 456

To specify a resource in a policy statement, in Amazon EC2, can you use its Amazon Resource Name (ARN)?

- A. Yes, you can.
- B. No, you can't because EC2 is not related to ARN.
- C. No, you can't because you can't specify a particular Amazon EC2 resource in an IAM policy.
- D. Yes, you can but only for the resources that are not affected by the action.

Answer: A

Explanation:

Some Amazon EC2 API actions allow you to include specific resources in your policy that can be created or modified by the action. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN).

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf>

QUESTION: 457

After you recommend Amazon Redshift to a client as an alternative solution to paying data warehouses to analyze his data, your client asks you to explain why you are recommending Redshift. Which of the following would be a reasonable response to his request?

- A. It has high performance at scale as data and query complexity grows.
- B. It prevents reporting and analytic processing from interfering with the performance of OLTP workloads.
- C. You don't have the administrative burden of running your own data warehouse and dealing with setup, durability, monitoring, scaling, and patching.
- D. All answers listed are a reasonable response to his question

Answer: D

Explanation:

Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host. AWS recommends Amazon Redshift for customers who have a combination of needs, such as: High performance at scale as data and query complexity grows Desire to prevent reporting and analytic processing from interfering with the performance of OLTP workloads Large volumes of structured data to persist and query using standard SQL and existing BI tools

Desire to the administrative burden of running one's own data warehouse and dealing with setup, durability, monitoring, scaling and patching
Reference: https://aws.amazon.com/running_databases/#redshift_anchor

QUESTION: 458

One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

- A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.
- B. Gateway-cached is free whilst gateway-stored is not.
- C. Gateway-cached is up to 10 times faster than gateway-stored.
- D. Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.
Gateway-cached enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

Answer: A

Explanation:

Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:

Gateway-cached volumes ?You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data. Gateway-stored volumes ?If you need low-latency access to your entire data set, you can configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

Reference: <http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html>

QUESTION: 459

A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

- A. Always select the AZ while launching an instance
- B. Always select the US-East-1-a zone for HA
- C. Do not select the AZ; instead let AWS select the AZ

- D. The user can never select the availability zone while launching an instance

Answer: C

Explanation:

When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>

QUESTION: 460

A user is storing a large number of objects on AWS S3. The user wants to implement the search functionality among the objects. How can the user achieve this?

- A. Use the indexing feature of S3.
- B. Tag the objects with the metadata to search on that.
- C. Use the query functionality of S3.
- D. Make your own DB system which stores the S3 metadata for the search functionality.

Answer: D

Explanation:

In Amazon Web Services, AWS S3 does not provide any query facility. To retrieve a specific object the user needs to know the exact bucket / object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping.

Reference: http://media.amazonaws.com/AWS_Storage_Options.pdf

QUESTION: 461

After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

- A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.

- B. A placement group can span multiple Availability Zones.
- C. You can't move an existing instance into a placement group.
- D. A placement group can span peered VPCs

Answer: B

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.

Placement groups have the following limitations:

The name you specify for a placement group a name must be unique within your AWS account. A placement group can't span multiple Availability Zones. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the same instance type for all instances in a placement group. You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group. A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide. You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

QUESTION: 462

What is a placement group in Amazon EC2?

- A. It is a group of EC2 instances within a single Availability Zone.
- B. It the edge location of your web content.
- C. It is the AWS region where you run the EC2 instance of your web content.
- D. It is a group used to span multiple Availability Zones.

Answer: A

Explanation:

A placement group is a logical grouping of instances within a single Availability Zone.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

QUESTION: 463

You are migrating an internal server on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

- A. to a 2TB EBS volume
- B. to an S3 bucket with 2 objects of 1TB
- C. to an 500GB EBS volume
- D. to an S3 bucket as a 2TB snapshot

Answer: B

Explanation:

An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.

Reference: <http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html>

QUESTION: 464

A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, software patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle database. Which of the following AWS databases would be best for accomplishing this task?

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

Answer: A

Explanation:

Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery.

Reference: <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>

QUESTION: 465

True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.

- A. This is true only if requested during the set-up of VPC.
- B. This is true.
- C. This is false.
- D. This is true only for US regions.

Answer: C

Explanation:

A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.

Reference: <https://aws.amazon.com/vpc/faqs/>

QUESTION: 466

An edge location refers to which Amazon Web Service?

- A. An edge location is referred to the network configured within a Zone or Region
- B. An edge location is an AWS Region
- C. An edge location is the location of the data center used for Amazon CloudFront.
- D. An edge location is a Zone within an AWS Region

Answer: C

Explanation:

Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site's logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin server - CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser's request does not have a copy of the file.

Reference: <http://aws.amazon.com/cloudfront/>

QUESTION: 467

Does DynamoDB support in-place atomic updates?

- A. Yes
- B. No
- C. It does support in-place non-atomic updates
- D. It is not defined

Answer: A

Explanation:

DynamoDB supports in-place atomic updates.

Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#WorkingWithItems.AtomicCounters>

QUESTION: 468

Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectivity between these remote offices?

- A. Amazon CloudFront
- B. AWS Direct Connect
- C. AWS CloudHSM
- D. AWS VPN CloudHub

Answer: D

Explanation:

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices. Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION: 469

In Amazon AWS, which of the following statements is true of key pairs?

- A. Key pairs are used only for Amazon SDKs.
- B. Key pairs are used only for Amazon EC2 and Amazon CloudFront.
- C. Key pairs are used only for Elastic Load Balancing and AWS IAM.
- D. Key pairs are used for all Amazon services.

Answer: B

Explanation:

Key pairs consist of a public and private key, where you use the private key to create a digital

signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Reference: <http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

QUESTION: 470

Does Amazon DynamoDB support both increment and decrement atomic operations?

- A. Only increment, since decrement are inherently impossible with DynamoDB's data model.
- B. No, neither increment nor decrement operations.
- C. Yes, both increment and decrement operations.
- D. Only decrement, since increment are inherently impossible with DynamoDB's data model.

Answer: C

Explanation:

Amazon DynamoDB supports increment and decrement atomic operations. Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html>

QUESTION: 471

An organization has three separate AWS accounts, one each for development, testing, and production. The organization wants the testing team to have access to certain AWS resources in the production account. How can the organization achieve this?

- A. It is not possible to access resources of one account with another account.
- B. Create the IAM roles with cross account access.
- C. Create the IAM user in a test account, and allow it access to the production environment with the IAM policy.
- D. Create the IAM users with cross account access.

Answer: B

Explanation:

An organization has multiple AWS accounts to isolate a development environment from a testing or production environment. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the IAM role with cross account access will provide a solution. Cross account access lets one account share access to their resources with users in the other AWS accounts.

Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION: 472

You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend you use to accomplish this?

- A. Oracle export/import utilities
- B. Oracle SQL Developer
- C. Oracle Data Pump
- D. DBMS_FILE_TRANSFER

Answer: C

Explanation:

How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database. For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use Oracle Data Pump to import complex databases or databases that are several hundred megabytes or several terabytes in size.

Reference:

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html>

QUESTION: 473

A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

- A. 950
- B. 990
- C. 1000
- D. 900

Answer: D

Explanation:

As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.

Reference: <http://aws.amazon.com/ec2/faqs/>

QUESTION: 474

You need to migrate a large amount of data into the cloud that you have stored on a hard disk and you decide that the best way to accomplish this is with AWS Import/Export and you mail the hard disk to AWS. Which of the following statements is incorrect in regards to AWS Import/Export?

- A. It can export from Amazon S3
- B. It can Import to Amazon Glacier
- C. It can export from Amazon Glacier.
- D. It can Import to Amazon EBS

Answer: C

Explanation:

AWS Import/Export supports:

Import to Amazon S3
Export from Amazon S3
Import to Amazon EBS
Import to Amazon
Glacier

AWS Import/Export does not currently support export from Amazon EBS or Amazon Glacier. Reference:

<https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html>

QUESTION: 475

You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like Route 53 to direct traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

- A. Route 53 doesn't support ELB with an internal health check. You need to create your own Route 53 health check of the ELB
- B. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.

- C. Route 53 doesn't support ELB with an internal health check. You need to associate your resource record set for the ELB with your own health check
- D. Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

Answer: D

Explanation:

With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly. When you enable this feature, Route 53 uses health checks--regularly making Internet requests to your application's endpoints from multiple locations around the world--to determine whether each endpoint of your application is up or down. To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB.

Reference: <http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dns-failover/>

QUESTION: 476

A user wants to use an EBS-backed Amazon EC2 instance for a temporary job. Based on the input data, the job is most likely to finish within a week. Which of the following steps should be followed to terminate the instance automatically once the job is finished?

- A. Configure the EC2 instance with a stop instance to terminate it.
- B. Configure the EC2 instance with ELB to terminate the instance when it remains idle.
- C. Configure the CloudWatch alarm on the instance that should perform the termination action once the instance is idle.
- D. Configure the Auto Scaling schedule activity that terminates the instance after 7 days.

Answer: C

Explanation:

Auto Scaling can start and stop the instance at a pre-defined time. Here, the total running time is unknown. Thus, the user has to use the CloudWatch alarm, which monitors the CPU utilization. The user can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. When the utilization is below the threshold limit, it will terminate the instance as a part of the instance action. Reference:

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html>

QUESTION: 477

Which of the following is true of Amazon EC2 security group?

- A. You can modify the outbound rules for EC2-Classic.
- B. You can modify the rules for a security group only if the security group controls the traffic for just one instance.
- C. You can modify the rules for a security group only when a new instance is created.
- D. You can modify the rules for a security group at any time.

Answer: D

Explanation:

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

Reference: <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html>

QUESTION: 478

An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default how many EIPs is each AWS account limited to on a per region basis?

- A. 1
- B. 5
- C. Unlimited
- D. 10

Answer: B

Explanation:

By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.

If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2 Elastic IP Address Request Form and give reasons as to your need for additional addresses.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-adressing-limit>

QUESTION: 479

In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

- A. Data is deleted from the instance store for security reasons.
- B. Data persists in the instance store.
- C. Data is partially present in the instance store.
- D. Data in the instance store will be lost.

Answer: B

Explanation:

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists.

However, data on instance store volumes is lost under the following circumstances.

Failure of an underlying drive

Stopping an Amazon EBS-backed instance

Terminating an instance

Reference:

<http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

QUESTION: 480

You are setting up a VPC and you need to set up a public subnet within that VPC. Which following requirement must be met for this subnet to be considered a public subnet?

- A. Subnet's traffic is not routed to an internet gateway but has its traffic routed to a virtual private gateway.
- B. Subnet's traffic is routed to an internet gateway.
- C. Subnet's traffic is not routed to an internet gateway.
- D. None of these answers can be considered a public subnet.

Answer: B

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources,

such as Amazon EC2 instances, into your VPC. You can configure your VPC: you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the Internet. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a VPN-only subnet.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION481

Can you specify the security group that you created for a VPC when you launch an instance in EC2-Classic?

- A. No, you can specify the security group created for EC2-Classic when you launch a VPC instance.
- B. No
- C. Yes
- D. No, you can specify the security group created for EC2-Classic to a non-VPC based instance only.

Answer: B

Explanation:

If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. When you launch an instance in EC2-Classic, you must specify a security group in the same region as the instance. You can't specify a security group that you created for a VPC when you launch an instance in EC2-Classic.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic-security-groups>

QUESTION: 482

You are checking the workload on some of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes and it seems that the I/O latency is higher than you require. You should probably check the _____ to make sure that your application is not trying to drive more IOPS than you have provisioned.

- A. Amount of IOPS that are available
- B. Acknowledgement from the storage subsystem
- C. Average queue length
- D. Time it takes for the I/O operation to complete

Answer: C

Explanation:

In EBS workload demand plays an important role in getting the most out of your General Purpose (SSD) and Provisioned IOPS (SSD) volumes. In order for your volumes to deliver the amount of IOPS that are available, they need to have enough I/O requests sent to them. There is a relationship between the demand on the volumes, the amount of IOPS that are available to them, and the latency of the request (the amount of time it takes for the I/O operation to complete).

Latency is the true end-to-end client time of an I/O operation; in other words, when the client sends a IO, how long does it take to get an acknowledgement from the storage subsystem that the IO read or write is complete.

If your I/O latency is higher than you require, check your average queue length to make sure that your application is not trying to drive more IOPS than you have provisioned. You can maintain high IOPS while keeping latency down by maintaining a low average queue length (which is achieved by provisioning more IOPS for your volume).

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html>

QUESTION: 483

You have been given a scope to deploy some AWS infrastructure for a large organisation. The requirements are that you will have a lot of EC2 instances but may need to add more when the average utilization of your Amazon EC2 fleet is high and conversely remove them when CPU utilization is low. Which AWS services would be best to use to accomplish this?

- A. Auto Scaling, Amazon CloudWatch and AWS Elastic Beanstalk
- B. Auto Scaling, Amazon CloudWatch and Elastic Load Balancing.
- C. Amazon CloudFront, Amazon CloudWatch and Elastic Load Balancing.
- D. AWS Elastic Beanstalk , Amazon CloudWatch and Elastic Load Balancing.

Answer: B

Explanation:

Auto Scaling enables you to follow the demand curve for your applications closely, reducing the need to manually provision Amazon EC2 capacity in advance. For example, you can set a condition to add new Amazon EC2 instances in increments to the Auto Scaling group when the average utilization of your Amazon EC2 fleet is high; and similarly, you can set a condition to remove instances in the same increments when CPU utilization is low. If you have predictable load changes, you can set a schedule through Auto Scaling to plan your scaling activities. You can use Amazon CloudWatch to send alarms to trigger scaling activities and Elastic Load Balancing to help distribute traffic to your instances within Auto Scaling groups. Auto Scaling enables you to run your Amazon EC2 fleet at optimal utilization.

Reference: <http://aws.amazon.com/autoscaling/>

QUESTION: 484

You are building infrastructure for a data warehousing solution and an extra request has come through that there will be a lot of business reporting queries running all the time and you are not sure if your current DB instance will be able to handle it. What would be the best solution for this?

- A. DB Parameter Groups
- B. Read Replicas
- C. Multi-AZ DB Instance deployment
- D. Database Snapshots

Answer: B

Explanation:

Read Replicas make it easy to take advantage of MySQL's built-in replication functionality to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. There are a variety of scenarios where deploying one or more Read Replicas for a given source DB Instance may make sense. Common reasons for deploying a Read Replica include:

Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more Read Replicas. Serving read traffic while the source DB Instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replica(s). For this use case, keep in mind that the data on the Read Replica

may be "stale" since the source DB Instance is unavailable. Business reporting or data warehousing scenarios; you may want business reporting queries to run against a Read Replica, rather than your primary, production DB Instance.

Reference: <https://aws.amazon.com/rds/faqs/>

QUESTION: 485

In DynamoDB, could you use IAM to grant access to Amazon DynamoDB resources and API actions?

- A. In DynamoDB there is no need to grant access
- B. Depended to the type of access
- C. No
- D. Yes

Answer: D

Explanation:

Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to

grant. You then attach that policy to an AWS IAM user or role.

Reference:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html>

QUESTION: 486

Much of your company's data does not need to be accessed often, and can take several hours for retrieval time, so it's stored on Amazon Glacier. However someone within your organization has expressed concerns that his data is more sensitive than the other data, and is wondering whether the high level of encryption that he knows is on S3 is also used on the much cheaper Glacier service. Which of the following statements would be most applicable in regards to this concern?

- A. There is no encryption on Amazon Glacier, that's why it is cheaper.
- B. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3 but you can change it to AES-256 if you are willing to pay more.
- C. Amazon Glacier automatically encrypts the data using AES-256, the same as Amazon S3.
- D. Amazon Glacier automatically encrypts the data using AES-128 a lesser encryption method than Amazon S3.

Answer: C

Explanation:

Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where S3 is designed for rapid retrieval, Glacier is meant to be used as an archival service for data that is not accessed often, and for which retrieval times of several hours are suitable. Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.99999999% for an archive. It stores each archive in multiple facilities and multiple devices. Unlike traditional systems which can require laborious data verification and manual repair, Glacier performs regular, systematic data integrity checks, and is built to be automatically self-healing.

Reference: <http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf>

QUESTION: 487

Your EBS volumes do not seem to be performing as expected and your team leader has requested you look into improving their performance. Which of the following is not a true

statement relating to the performance of your EBS volumes?

- A. Frequent snapshots provide a higher level of data durability and they will not degrade the performance of your application while the snapshot is in progress.
- B. General Purpose (SSD) and Provisioned IOPS (SSD) volumes have a throughput limit of 128 MB/s per volume.

- C. There is a relationship between the maximum performance of your EBS volumes, the amount of I/O you are driving to them, and the amount of time it takes for each transaction to complete.
- D. There is a 5 to 50 percent reduction in IOPS when you first access each block of data on a newly created or restored EBS volume

Answer: A

Explanation:

Several factors can affect the performance of Amazon EBS volumes, such as instance configuration, I/O characteristics, workload demand, and storage configuration. Frequent snapshots provide a higher level of data durability, but they may slightly degrade the performance of your application while the snapshot is in progress. This trade off becomes critical when you have data that changes rapidly. Whenever possible, plan for snapshots to occur during off-peak times in order to minimize workload impact.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html>

QUESTION: 48\8

A major finance organisation has engaged your company to set up a large data mining application. Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop. Which of the following statements best describes Hadoop?

- A. Hadoop is 3rd Party software which can be installed using AMI
- B. Hadoop is an open source python web framework
- C. Hadoop is an open source Java software framework
- D. Hadoop is an open source javascript framework

Answer: C

Explanation:

Amazon EMR uses Apache Hadoop as its distributed data processing engine. Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named "MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster.

This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.

Reference: <http://aws.amazon.com/elasticmapreduce/faqs/>

QUESTION: 489

In Amazon EC2 Container Service, are other container types supported?

- A. Yes, EC2 Container Service supports any container service you need.
- B. Yes, EC2 Container Service also supports Microsoft container service.
- C. No, Docker is the only container platform supported by EC2 Container Service presently.
- D. Yes, EC2 Container Service supports Microsoft container service and Openstack.

Answer: C

Explanation:

In Amazon EC2 Container Service, Docker is the only container platform supported by EC2 Container Service presently.

Reference: <http://aws.amazon.com/ecs/faqs/>

QUESTION: 490

A Solutions Architect is designing the architecture for a web application that will be hosted on AWS. Internet users will access the application using HTTP and HTTPS.

How should the Architect design the traffic control requirements?

- A. Use a network ACL to allow outbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
- B. Use a network ACL to allow inbound ports for HTTP and HTTPS. Deny other traffic for inbound and outbound.
- C. Allow inbound ports for HTTP and HTTPS in the security group used by the webservers.
- D. Allow outbound ports for HTTP and HTTPS in the security group used by the webservers.

Answer: C

QUESTION: 491

A company built a food ordering application that captures user data and stores it for future analysis.

The application's static front end is deployed on an Amazon EC2 instance.

The front-end application sends the requests to the backend application running on separate EC2 instance.

The backend application then stores the data in Amazon RDS

What should a solutions architect do to decouple the architecture and make it scalable?"

- A. Use Amazon S3 to serve the front-end application which sends requests to Amazon EC2 to execute the backend application.
The backend application will process and store the data in Amazon RDS
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic.
Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic and process and store the data in Amazon RDS
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue.
Place the backend instance in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway which writes the requests to an Amazon SQS queue.
Place the backend instances in an Auto Scaling group and scale based on the queue depth to process and store the data in Amazon RDS

Answer: D

Explanation

Keyword: Static + Decouple + Scalable

Static=S3

Decouple=SQS Queue

Scalable=ASG

Option B will not be there in the race due to Auto-Scaling unavailability. Option A will not be there in the race due to Decouple unavailability.

Option C & D will be in the race and Option D will be correct answers due to all 3 combination matches [Static=S3; Decouple=SQS Queue; Scalable=ASG] & Option C will loose due to Static option unavailability

QUESTION: 492

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention. Which solution should a solution architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and amazon Aura Global for datastorage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Answer: B

QUESTION: 493

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 it uses to store data. Some of the S3 bucket have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage. Which solution will lower costs without compromising the availability of objects?

- A. Use S3 ACLs
- B. Use Amazon Elastic Block Store (EBS) automated snapshots
- C. Use S3 Intelligent-Tiering storage
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Answer: C

QUESTION: 494

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances. What should a solution architect do to accomplish this?

- A. Configure a volume using Amazon EFS Mount the EFS volume to each Windows instance
- B. Configure AWS Storage Gateway in Volume Gateway mode Mount the volume to each Windows instance
- C. Configure Amazon FSx for Windows File Server Mount the Amazon FSx volume to each Windows instance
- D. Configure an Amazon EBS volume with the required size Attach each EC2 instance to the volume Mount the file system within the volume to each Windows instance

Answer: C

_r53

QUESTION: 495

A company's operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.

Which solution would satisfy these requirements?

- A. Create another SQS queue Update the S3 events in bucket to also update the new queue when a new object is created.
- B. Create a new SQS queue that only allows Amazon S3 to access the queue, Update Amazon S3 update this queue when a new object is created
- C. Create an Amazon SNS topic and SQS queue for the Update. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
- D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic Add subscription for both queue in the topic.

Answer: D

QUESTION: 496

An ecommerce company has noticed performance degradation of its Amazon RDS based web application.

The performance degradation is attribute to an increase in the number of read-only SQL queries triggered by business analysts.

A solution architect needs to solve the problem with minimal changes to the existing web application.

What should the solution architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElasticCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Answer: C

QUESTION: 497

A company has migrated an on-premises Oracle database to an Amazon RDS (or Oracle Multi-AZ DB instance In the us-east-1 Region).

A solutions architect is designing a disaster recovery strategy to have the database provisioned In the us-west-2 Region In case the database becomes unavailable in the us-east-1 Region.

The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

- A. Edit the DB instance and create a read replica in us-west-2.
Promote the read replica to master In us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2.
The standby Instance will be automatically promoted to master In us-west-2 in case the

- disaster recovery environment needs to be created.
- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
 - D. Create a multimaster read/write instances across multiple AWS Regions Select VPCs in us-east-1 and us-west-2 to make that deployment.
Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Answer: A

QUESTION: 498

A company is moving its legacy workload to the AWS Cloud.
The workload files will be shared, appended, and frequently accessed through Amazon EC2 instances when they are first created.

The files will be accessed occasionally as they age
What should a solutions architect recommend?

- A. Store the data using Amazon EC2 instances with attached Amazon Elastic Block Store (Amazon EBS) data volumes
- B. Store the data using AWS Storage Gateway volume gateway and export rarely accessed data to Amazon S3 storage
- C. Store the data using Amazon Elastic File System (Amazon EFS) with lifecycle management enabled for rarely accessed data
- D. Store the data using Amazon S3 with an S3 lifecycle policy enabled to move data to S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: D

QUESTION: 499

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set
- B. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set to private
- C. Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set

Answer: D

QUESTION: 500

An engineering team is developing and deploying AWS Lambda functions.
The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.

How should the permissions for the team be configured so they also adhere to the concept of least privilege?

- A. Create an IAM role with a managed policy attached.
Allow the engineering team and the Lambda functions to assume this role
- B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group
- C. Create an execution role for the Lambda functions.
Attach a managed policy that has permission boundaries specific to these Lambda functions
- D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions.
Allow the engineering team to assume this role.

Answer: D

QUESTION: 501

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application.

The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern.

The solutions architect must minimize the costs of storing and retrieving the media files. Which storage option meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Answer: B

QUESTION: 502

A company is designing a message-driven order processing application on AWS.

The application consists of many services and needs to communicate the results of its processing to multiple consuming services.

Each of the consuming services may take up to 5 days to receive the messages.

Which process will meet these requirements?

- A. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
Each consuming service subscribes to this SNS topic and consumes the results
- B. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
Each consuming service consumes the messages directly from its corresponding SNS topic.
- C. The application sends the results of its processing to an Amazon Simple Queue Service (Amazon SQS) queue.
Each consuming service runs as an AWS Lambda function that consumes this single SQS queue.
- D. The application sends the results of its processing to an Amazon Simple Notification Service (Amazon SNS) topic.
An Amazon Simple Queue Service (Amazon SQS) queue is created for each service and each queue is configured to be a subscriber of the SNS topic.

Answer: C

QUESTION: 503

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service free and paid Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS. Which configuration should a solutions architect recommend?

- A. Use one SQS FIFO queue.
Assign a higher priority to the paid photos so they are processed first
- B. Use two SQS FIFO queues: one for paid and one for free.
Set the free queue to use short polling and the paid queue to use long polling
- C. Use two SQS standard queues one for paid and one for free.
Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
- D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero.
Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first

Answer: C

QUESTION: 504

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions.

To communicate with each other, the instances use the internet for connectivity.

The security team wants to ensure that no communication between the instances happens over the internet.

What should a solutions architect do to accomplish this?"

- A. Create a NAT gateway and update the route table of the EC2 instances'subnet
- B. Create a VPC endpoint and update the route table of the EC2 instances'subnet
- C. Create a VPN connection and update the route table of the EC2 instances'subnet
- D. Create a VPC peering connection and update the route table of the EC2 instances'subnet

Answer: D

QUESTION: 505

A company runs a production application on a fleet of Amazon EC2 instances.

The application reads the data from an Amazon SQS queue and processes the messages in parallel.

The message volume is unpredictable and often has intermittent traffic.

This application should continually process messages without any downtime Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required
- B. Use Reserved Instances exclusively to handle the maximum capacity required
- C. Use Reserved Instances for the baseline capacity and use Spot InstaKes to handle additional capacity

- D. Use Reserved instances for the baseline capacity and use On-Demand Instances to handle additional capacity

Answer: D

Explanation:



EC2 Spot Instances

- Can get a discount of up to 90% compared to On-demand
- Instances that you can "lose" at any point of time if your max price is less than the current spot price
- The MOST cost-efficient instances in AWS
- Useful for workloads that are resilient to failure
 - Batch jobs
 - Data analysis
 - Image processing
 - ...
- Not great for critical jobs or databases
- Great combo: Reserved Instances for baseline + On-Demand & Spot for peaks

QUESTION: 506

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly.

Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

- A. Create an additional NAT gateway Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic
- B. Create an internet gateway Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3 Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Answer: C

QUESTION: 507

A solution architect is designing a shared storage solution for an Auto Scaling web application. The company anticipates making frequent changes to the content, so the solution must have strong consistency.

Which solution requires the LEAST amount of effort?

- A. Create an Amazon S3 bucket to store the web content and use Amazon Cloudfront to deliver the content
- B. Create an Amazon Elastic File system (Amazon EFS) file system and mount it on the individual Amazon EC2 instance
- C. Create a shared Amazon Elastic Block store (Amazon EBS) volume and mount it on the individual Amazon EC2 instance
- D. Use AWS Datasync to perform continuous synchronization of data between Amazon EC2 hosts in the Auto scaling group.

Answer: B

QUESTION: 508

A company uses a legacy on-premises analytics application that operate on gigabytes of .csv and represents months of data. The legacy application cannot handle the growing size of .csv files.

New CSV files added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while user learn AWS analytics services. To achieve this, a solution architect wants to maintain two synchronizes copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solution architect recommend?

- A. Deploy AWS Datasync on-premises. Configure Datasync to continuously replicate the .csv files between the company's S3 bucket.
- B. Deploy an on-premises file gateway. Configure data source to write the .csv files to the file gateway, point the legacy analytics application to the file gateway.
The file gateway should replicate the .csv file to Amazon S3.
- C. Deploy an on-premises volume gateway. Configure data source to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway.
The volume gateway should replicate data to Amazon S3.
- D. Deploy AWS Datasync on-premises. Configure Datasync to continuously replicate the .csv files between on-premises and Amazon Elastic file system (Amazon EFS) enable replication from Amazon EFS to the company's S3 Bucket.

Answer: A

QUESTION: 509

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.

What should a solutions architect recommend?

- A. Set up a new Direct Connect connection in another AWS Region.
- B. Set up a new AWS managed VPN connection in another AWS Region.
- C. Set up two new Direct Connect connections one in the current AWS Region and one in another Region.
- D. Set up two new AWS managed VPN connections one in the current AWS Region and one in another Region.

Answer: A

QUESTION: 510

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center. This backup data needs to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migrations must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

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

<https://itexamcertified.com>

Answer: A

QUESTION: 511

A application running on an Amazon EC2 instance needs to securely access files on an Amazon Elastic File System (Amazon EFS) file system. The EFS files are stores using encryptions at rest.

Which solution for accessing teh files in MOST secure?

- A. Enable TLS when mounting Amazon EFS.
- B. Store the encryption key in the code of the application.
- C. Enable AWS Key MAnagement Service (AKS KMS) when mounting Amazon EFS.
- D. Store the encryption key in an Amazon S3 bucket and use IAM roles to grand the EC2 instance access permission.

Answer: C

QUESTION: 512

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR block as the source or destination.
- D. Create security group rules using the subnet CIDR block as the source or destination.

Answer: B

QUESTION: 513

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

<https://itexamcertified.com>

Which solution meets these requirements?

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

Answer: B

QUESTION: 514

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content to meet the migration date, minimal changes can be made.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web server.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
- D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPSSSD (io1) volumes and mount them on all web servers.

Answer: C

QUESTION: 515

A company runs an application on an Amazon EC2 instance Backed by Amazon Elastic Block Store (Amazon EBS).

The instance needs to be available for 12 hours daily.

The company wants to save costs by making the instance unavailable outside the window required for the application.

However the contents of the instance's memory must be preserved whenever the instance is unavailable.

What should a solutions architect do to meet this requirement?

- A. Stop the instance outside the application's availability window. Start up the Instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again

- when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
 - D. Terminate the instance outside the application's availability window.
Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Answer: B

QUESTION: 516

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently. How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Answer: A

QUESTION: 517

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company's account. All the needed policies have been created to grant appropriate access.

Which additional component will provide the vendor with the MOST secure access to the account?

- A. Create an IAM user.
- B. Implement a service control policy (SCP)
- C. Use a cross-account role with an external ID.

- D. Configure a single sign-on (SSO) identity provider.

Answer: C

QUESTION: 518

A solutions architect must design a database solution for a high-traffic ecommerce web application. The database stores customer profiles and shopping cart information. The database must support a peak load of several million requests each second and deliver responses in milliseconds. The operational overhead for managing and scaling the database must be minimized. Which database solution should the solutions architect recommend?

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

Answer: A

Question #519

A company is migrating its applications to AWS. Currently, applications that run on premises generate hundreds of terabytes of data that is stored on a shared file system. The company is running an analytics application in the cloud that runs hourly to generate insights from this data.

The company needs a solution to handle the ongoing data transfer between the on-premises shared file system and Amazon S3. The solution also must be able to handle occasional interruptions in internet connectivity.

Which solutions should the company use for the data transfer to meet these requirements?

- A. AWS DataSync
- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

Correct Answer: A

Reference:

<https://itexamcertified.com>

<https://aws.amazon.com/cloud-data-migration/>

Question #520

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load

Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database.

What should the solutions architect do to ensure that the website can scale with increasing traffic? (Choose two.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Correct Answer: BE

Question #521

A company captures ordered clickstream data from multiple websites and uses batch processing to analyze the data. The company receives 100 million event records, all approximately 1 KB in size, each day. The company loads the data into Amazon Redshift each night, and business analysts consume the data.

The company wants to move toward near-real-time data processing for timely insights. The solution should process the streaming data while requiring the least possible operational overhead.

Which combination of AWS services will meet these requirements MOST cost-effectively? (Choose two.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose

<https://itexamcertified.com>

E. Amazon Kinesis Data Analytics

Correct Answer: CE

Question #522

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company's IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.

What should a solutions architect do to secure the data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Correct Answer: C

Question #523

A company with a single AWS account runs its internet-facing containerized web application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

The EKS cluster is placed in a private subnet of a VPC. System administrators access the EKS cluster through a bastion host on a public subnet.

A new corporate security policy requires the company to avoid the use of bastion hosts. The company also must not allow internet connectivity to the EKS cluster.

Which solution meets these requirements MOST cost-effectively?

- A. Set up an AWS Direct Connect connection.
- B. Create a transit gateway.
- C. Establish a VPN connection.
- D. Use AWS Storage Gateway.

Correct Answer: B

Question #524

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Correct Answer: C

Question #525

A company is migrating a large, mission-critical database to AWS. A solutions architect has decided to use an Amazon RDS for MySQL Multi-AZ DB instance that is deployed with 80,000 Provisioned IOPS for storage. The solutions architect is using AWS Database Migration Service (AWS DMS) to perform the data migration. The migration is taking longer than expected, and the company wants to speed up the process. The company's network team has ruled out bandwidth as a limiting factor.

Which actions should the solutions architect take to speed up the migration? (Choose two.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

Correct Answer: CD

Question #526

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
- B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
- C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
- D. Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Correct Answer: C

Question #527

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these

VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Correct Answer: D

Question #528

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.

Which combination of network solutions will meet these requirements? (Choose two.)

- A. Enable and configure enhanced networking on each EC2 instance.
- B. Group the EC2 instances in separate accounts.
- C. Run the EC2 instances in a cluster placement group.
- D. Attach multiple elastic network interfaces to each EC2 instance.
- E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Correct Answer: CD

Question #529

A company is running a global application. The application's users submit multiple videos that are then merged into a single video file. The application uses a single Amazon S3 bucket in the us-east-1 Region to receive uploads from users. The same S3 bucket provides the download location of the single video file that is produced. The final video file output has an average size of 250 GB.

The company needs to develop a solution that delivers faster uploads and downloads of the video files that are stored in Amazon S3. The company will offer the solution as a subscription to users who want to pay for the increased speed.

What should a solutions architect do to meet these requirements?

- A. Enable AWS Global Accelerator for the S3 endpoint. Adjust the application's upload and download links to use the Global Accelerator S3 endpoint for users who have a subscription.
- B. Enable S3 Cross-Region Replication to S3 buckets in all other AWS Regions. Use an Amazon Route 53 geolocation routing policy to route S3 requests based on the location of users who have a subscription.
- C. Create an Amazon CloudFront distribution and use the S3 bucket in us-east-1 as an origin. Adjust the application to use the CloudFront URL as the upload and download links for users who have a subscription.

D. Enable S3 Transfer Acceleration for the S3 bucket in us-east-1. Configure the application to use the bucket's S3-accelerate endpoint domain name for the upload and download links for users who have a subscription.

Correct Answer: C

Question #530

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "1",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        }  
    ]  
}
```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).

C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.

D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Correct Answer: D

Question #531

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: A

Question #532

A company is using AWS Organizations with two AWS accounts: Logistics and Sales. The Logistics account operates an Amazon Redshift cluster. The Sales account includes Amazon EC2 instances. The Sales account needs to access the Logistics account's Amazon Redshift cluster.

What should a solutions architect recommend to meet this requirement MOST cost-effectively?

- A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data.
- B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account.

<https://itexamcertified.com>

C. Create a snapshot of the Amazon Redshift cluster, and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account.

D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account.

Correct Answer: C

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>

Question #533

A company is using Amazon Redshift for analytics and to generate customer reports. The company recently acquired 50 TB of additional customer demographic data. The data is stored in .csv files in Amazon S3. The company needs a solution that joins the data and visualizes the results with the least possible cost and effort.

What should a solutions architect recommend to meet these requirements?

- A. Use Amazon Redshift Spectrum to query the data in Amazon S3 directly and join that data with the existing data in Amazon Redshift. Use Amazon QuickSight to build the visualizations.
- B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSight to join the data from Athena with the existing data in Amazon Redshift and to build the visualizations.
- C. Increase the size of the Amazon Redshift cluster, and load the data from Amazon S3. Use Amazon EMR Notebooks to query the data and build the visualizations in Amazon Redshift.
- D. Export the data from the Amazon Redshift cluster into Apache Parquet files in Amazon S3. Use Amazon Elasticsearch Service (Amazon ES) to query the data. Use Kibana to visualize the results.

Correct Answer: A

Question #534

A solutions architect must provide a fully managed replacement for an on-premises solution that allows employees and partners to exchange files. The solution must be easily accessible to employees connecting from on-premises systems, remote employees, and external partners.

Which solution meets these requirements?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.

<https://itexamcertified.com>

- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Question #535

A company's database is hosted on an Amazon Aurora MySQL DB cluster in the us-east-1 Region. The database is 4 TB in size. The company needs to expand its disaster recovery strategy to the us-west-2 Region. The company must have the ability to fail over to us-west-2 with a recovery time objective (RTO) of 15 minutes.

What should a solutions architect recommend to meet these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Correct Answer: B

Reference:

<https://docs.aws.amazon.com/aws-backup/latest/devguide/eventbridge.html>

Question #536

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

- A. Use Amazon EC2 instances, and install Docker on the instances.
- B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.

<https://itexamcertified.com>

- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Answer: C

Reference:

<https://aws.amazon.com/fargate/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc&fargate-blogs.sort-by=item.additionalFields.createdDate&fargate-blogs.sort-order=desc>

Question #537

A company is designing a new application that runs in a VPC on Amazon EC2 instances. The application stores data in Amazon S3 and uses Amazon DynamoDB as its database. For compliance reasons, the company prohibits all traffic between the EC2 instances and other AWS services from passing over the public internet.

What can a solutions architect do to meet this requirement?

- A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB.
- B. Configure interface VPC endpoints to Amazon S3 and DynamoDB.
- C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.
- D. Configure a gateway VPC endpoint to DynamoDB. Configure an interface VPC endpoint to Amazon S3.

Answer: A

Question #538

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Answer: D

Question #539

<https://itexamcertified.com>

<https://itexamcertified.com>

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

Answer: B

Question #540

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

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

<https://itexamcertified.com>

<https://itexamcertified.com>

Answer: B

Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

Question #541

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on

AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

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

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Answer: AB

Question #542

A company recently launched a new service that involves medical images. The company scans the images and sends them from its on-premises data center through an AWS Direct Connect connection to Amazon EC2 instances. After processing is complete, the images are stored in an Amazon S3 bucket.

A company requirement states that the EC2 instances cannot be accessible through the internet. The EC2 instances run in a private subnet, which has a default route back to the on-premises data center for outbound internet access.

Usage of the new service is increasing rapidly. A solutions architect must recommend a solution that meets the company's requirements and reduces the Direct

Connect charges.

Which solution accomplishes these goals MOST cost-effectively?

- A. Configure a VPC endpoint for Amazon S3. Add an entry to the private subnet's route table for the S3 endpoint.

<https://itexamcertified.com>

- B. Configure a NAT gateway in a public subnet. Configure the private subnet's route table to use the NAT gateway.
- C. Configure Amazon S3 as a file system mount point on the EC2 instances. Access Amazon S3 through the mount.
- D. Move the EC2 instances into a public subnet. Configure the public subnet route table to point to an internet gateway.

Answer: B

Question #543

A company is building an online multiplayer game. The game communicates by using UDP, and low latency between the client and the backend is important. The backend is hosted on Amazon EC2 instances that can be deployed to multiple AWS Regions to meet demand. The company needs the game to be highly available so that users around the world can access the game at all times.

What should a solutions architect do to meet these requirements?

- A. Deploy Amazon CloudFront to support the global traffic. Configure CloudFront with an origin group to allow access to EC2 instances in multiple Regions.
- B. Deploy an Application Load Balancer in one Region to distribute traffic to EC2 instances in each Region that hosts the game's backend instances.
- C. Deploy Amazon CloudFront to support an origin access identity (OAI). Associate the OAI with EC2 instances in each Region to support global traffic.
- D. Deploy a Network Load Balancer in each Region to distribute the traffic. Use AWS Global Accelerator to route traffic to the correct Regional endpoint.

Answer: B

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

Question #544

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

<https://itexamcertified.com>

- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Answer: AB

Question #545

A security team needs to enforce the rotation of all IAM users' access keys every 90 days. If an access key is found to be older, the key must be made inactive and removed. A solutions architect must create a solution that will check for and remediate any keys older than 90 days.

Which solution meets these requirements with the LEAST operational effort?

- A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.
- C. Create an AWS Config rule to check for the key age. Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key.

Answer: A

Reference:

<https://aws.amazon.com/blogs/mt/managing-aged-access-keys-through-aws-config-remediations/>

Question #546

A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from

0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.

What should the solutions architect do to meet these requirements with the LEAST operational overhead?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.
- B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
- C. Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.
- D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

Answer: B

Reference:

<https://www.stratoscale.com/blog/compute/aws-security-groups-5-best-practices/>

Question #547

A media company is using two video conversion tools that run on Amazon EC2 instances. One tool runs on Windows instances, and the other tool runs on Linux instances. Each video file is large in size and must be processed by both tools.

The company needs a storage solution that can provide a centralized file system that can be mounted on all the EC2 instances that are used in this process.

Which solution meets these requirements?

- A. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.
- B. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.
- C. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances
- D. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.

Answer: BC

Question #548

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet.

An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.

<https://itexamcertified.com>

<https://itexamcertified.com>

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

- A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
- B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
- C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
- D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Answer: D

Question #549

A company is planning to migrate a TCP-based application into the company's VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company's data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Answer:A

Question #550

An ecommerce company is creating an application that requires a connection to a third-party payment service to process payments. The payment service needs to explicitly allow the public IP address of the server that is making the payment request. However, the company's security policies do not allow any server to be exposed directly to the public internet.

<https://itexamcertified.com>

<https://itexamcertified.com>

Which solution will meet these requirements?

- A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.
- B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.
- C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.
- D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

Answer: B

Question #551

A company is running an ASP.NET MVC application on a single Amazon EC2 instance. A recent increase in application traffic is causing slow response times for users during lunch hours. The company needs to resolve this concern with the least amount of configuration.

What should a solutions architect recommend to meet these requirements?

- A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours.
- B. Move the application to Amazon Elastic Container Service (Amazon ECS). Create an AWS Lambda function to handle scaling during lunch hours.
- C. Move the application to Amazon Elastic Container Service (Amazon ECS). Configure scheduled scaling for AWS Application Auto Scaling during lunch hours.
- D. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling, and create an AWS Lambda function to handle scaling during lunch hours.

Answer: A

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-scheduledactions.html>

Question #552

An online gaming company is designing a game that is expected to be popular all over the world. A solutions architect needs to define an AWS Cloud architecture that supports near-real-time recording and displaying of current game statistics for each player, along with the names of the top 25 players in the world, at any given time.

Which AWS database solution and configuration should the solutions architect use to meet these requirements?

<https://itexamcertified.com>

<https://itexamcertified.com>

- A. Use Amazon RDS for MySQL as the data store for player activity. Configure the RDS DB instance for Multi-AZ support.
- B. Use Amazon DynamoDB as the data store for player activity. Configure DynamoDB Accelerator (DAX) for the player data.
- C. Use Amazon DynamoDB as the data store for player activity. Configure global tables in each required AWS Region for the player data.
- D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-Region read replicas in each required AWS Region based on player proximity.

Answer: D

Question #553

A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases.

Which solution meets this requirement with the LEAST operational overhead?

- A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.
- B. Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.
- C. Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.
- D. Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the customer master key (CMK).

Answer: A

Reference -

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

Question #554

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.

<https://itexamcertified.com>

- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Answer: B

Question #555

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

- A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
- B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
- C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
- D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Answer: B

Question #556

A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application's code.

Which solution meets these requirements?

- A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
- B. Use Amazon EC2 instances to migrate and operate the database servers.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
- D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

<https://itexamcertified.com>

Answer: A

Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html>

Question #557

A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward.

The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application. The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.

The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs.

What should a solutions architect recommend to meet these requirements?

- A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
- B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.
- C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.
- D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

Answer: C

Question #558

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

Answer: C

<https://itexamcertified.com>

<https://itexamcertified.com>

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

559.

Question #559

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Correct Answer: B

Question #560

A company is running an application on AWS to process weather sensor data that is stored in an Amazon S3 bucket. Three batch jobs run hourly to process the data in the S3 bucket for different purposes. The company wants to reduce the overall processing time by running the three applications in parallel using an event-based approach.

What should a solutions architect do to meet these requirements?

- A. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Subscribe all applications to the queue for processing.
- B. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) standard queue. Create an additional SQS queue for all applications, and subscribe all applications to the initial queue for processing.

<https://itexamcertified.com>

<https://itexamcertified.com>

C. Enable S3 Event Notifications for new objects to separate Amazon Simple Queue Service (Amazon SQS) FIFO queues. Create an additional SQS queue for each application, and subscribe each queue to the initial topic for processing.

D. Enable S3 Event Notifications for new objects to an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon Simple Queue Service (Amazon SQS) queue for each application, and subscribe each queue to the topic for processing.

Correct Answer: D

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ways-to-add-notification-config-to-bucket.html>

Question #561

A company wants to use a custom distributed application that calculates various profit and loss scenarios. To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances. The connection must minimize latency and must maximize throughput

Which solution will meet these requirements?

- A. Provision the application to use EC2 Dedicated Hosts of the same instance type.
- B. Configure a placement group for EC2 instances that have the same instance type.
- C. Use multiple AWS elastic network interfaces and link aggregation.
- D. Configure AWS PrivateLink for the EC2 instances.

Correct Answer: B

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/network-throughput-benchmark-linux-ec2/>

Question #562

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
- D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

<https://itexamcertified.com>

<https://itexamcertified.com>

Correct Answer: D

Question #563

A company is relocating its data center and wants to securely transfer 58 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized.

Which AWS service should a solutions architect use to meet these requirements?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized
- D. AWS Storage Gateway

Correct Answer: C

Question #564

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.

What should a solutions architect recommend to meet this requirement?

- A. Use Amazon ElastiCache for Redis.
- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: B

Question #565

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications.

What should a solutions architect do to reduce the operational burden?

- A. Use multi-factor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.

<https://itexamcertified.com>

<https://itexamcertified.com>

D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Correct Answer: B

Reference:

<https://aws.amazon.com/kms/faqs/>

Question #566

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
- C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
- D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Correct Answer: A

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

Question #567

A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database. The company deploys Amazon EC2 instances to a private network to process data from the database. The company uses two NAT instances to provide connectivity to DynamoDB.

The company wants to retire the NAT instances. A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management.

What is the MOST cost-effective solution that meets these requirements?

- A. Create a gateway VPC endpoint to provide connectivity to DynamoDB.
- B. Configure a managed NAT gateway to provide connectivity to DynamoDB.
- C. Establish an AWS Direct Connect connection between the private network and DynamoDB.
- D. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB.

<https://itexamcertified.com>

<https://itexamcertified.com>

Correct Answer: A

Question #568

A solutions architect is designing a two-tiered architecture that has separate private subnets for compute resources and the database. An AWS Lambda function that is deployed in the compute subnets needs connectivity to the database.

Which solution will provide this connectivity in the MOST secure way?

- A. Configure the Lambda function to use Amazon RDS Proxy outside the VPC.
- B. Associate a security group with the Lambda function. Authorize this security group in the database's security group.
- C. Authorize the compute subnet's CIDR ranges in the database's security group.
- D. During the initialization phase, authorize all IP addresses in the database's security group temporarily. Remove the rule after the initialization is complete.

Correct Answer: B

Question #569

A ride-sharing company stores historical service usage data as structured .csv data files in Amazon S3. A data analyst needs to perform SQL queries on this data.

A solutions architect must recommend a solution that optimizes cost-effectiveness for the queries.

Which solution meets these requirements?

- A. Create an Amazon EMR cluster. Load the data. Perform the queries.
- B. Create an Amazon Redshift cluster. Import the data. Perform the queries.
- C. Create an Amazon Aurora PostgreSQL DB cluster. Import the data. Perform the queries.
- D. Create an Amazon Athena database. Associate the data in Amazon S3. Perform the queries.

Correct Answer: D

Reference:

<https://searchcloudcomputing.techtarget.com/answer/Compare-EMR-Redshift-and-Athena-for-data-analysis-on-AWS>

Question #570

<https://itexamcertified.com>

<https://itexamcertified.com>

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

- A. Create a usage plan with an API key that is shared with genuine users only.
- B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
- C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
- D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
- E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Correct Answer: AC

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

Question #571

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

What should the solutions architect do to maximize reliability of the application's infrastructure?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Correct Answer: B

Question #572

<https://itexamcertified.com>

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all existing and new photos in another geographical location.

Which solution will meet this requirement with the LEAST operational effort?

- A. Create a second S3 bucket in us-east-1. Enable S3 Cross-Region Replication from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle management rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1 to store the replicated photos. Configure S3 event notifications on object creation and update events that invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: A

Question #573

A company wants to migrate its accounting system from an on-premises data center to the AWS Cloud in a single AWS Region. Data security and an immutable audit log are the top priorities. The company must monitor all AWS activities for compliance auditing. The company has enabled AWS CloudTrail but wants to make sure it meets these requirements.

Which actions should a solutions architect take to protect and secure CloudTrail? (Choose two.)

- A. Enable CloudTrail log file validation.
- B. Install the CloudTrail Processing Library.
- C. Enable logging of Insights events in CloudTrail.
- D. Enable custom logging from the on-premises resources.
- E. Create an AWS Config rule to monitor whether CloudTrail is configured to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS).

Correct Answer: AE

Question #574

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an

<https://itexamcertified.com>

Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

- A. Update the Kinesis Data Streams default settings by modifying the data retention period.
- B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Correct Answer: A

Reference:

<https://aws.amazon.com/kinesis/data-firehose/faqs/>

Question #575

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an

Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.

A solutions architect needs to design a solution that stores customer data that is created during database upgrades.

Which solution will meet these requirements?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Correct Answer: A

<https://itexamcertified.com>

Question #576

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon

CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.

What should a solutions architect do to meet these requirements?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
- C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Correct Answer: D

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/>

Question #577

A company has primary and secondary data centers that are 580 miles (804.7 km) apart and interconnected with high-speed fiber-optic cable. The company needs a highly available and secure network connection between its data centers and a VPC on AWS for a mission-critical workload. A solutions architect must choose a connection solution that provides maximum resiliency.

Which solution meets these requirements?

- A. Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
- B. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
- C. Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
- D. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Correct Answer: C

Question #578

<https://itexamcertified.com>

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Correct Answer: A

Reference:

Question #579

A company is hosting its website by using Amazon EC2 instances behind an Elastic Load Balancer across multiple Availability Zones. The instances run in an

EC2 Auto Scaling group. The website uses Amazon Elastic Block Store (Amazon EBS) volumes to store product manuals for users to download. The company updates the product content often, so new instances launched by the Auto Scaling group often have old data. It can take up to 30 minutes for the new instances to receive all the updates. The updates also require the EBS volumes to be resized during business hours.

The company wants to ensure that the product manuals are always up to date on all instances and that the architecture adjusts quickly to increased user demand.

A solutions architect needs to meet these requirements without causing the company to update its application code or adjust its website.

What should the solutions architect do to accomplish this goal?

- A. Store the product manuals in an EBS volume. Mount that volume to the EC2 instances.
- B. Store the product manuals in an Amazon S3 bucket. Redirect the downloads to this bucket.
- C. Store the product manuals in an Amazon Elastic File System (Amazon EFS) volume. Mount that volume to the EC2 instances.
- D. Store the product manuals in an Amazon S3 Standard-Infrequent Access (S3 Standard-IA) bucket. Redirect the downloads to this bucket.

Correct Answer: C

<https://itexamcertified.com>

Question #580

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in

Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide are accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Correct Answer: B

Reference:

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

Question #581

A company is building its web application by using containers on AWS. The company requires three instances of the web application to run at all times. The application must be highly available and must be able to scale to meet increases in demand.

Which solution meets these requirements?

- A. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
- B. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in three different Availability Zones. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
- D. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance. Place one task on the remaining container instance.

Correct Answer: C

Reference:

<https://itexamcertified.com>

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-placement.html>
<https://aws.amazon.com/blogs/containers/amazon-ecs-availability-best-practices/>

Question #582

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C

Question #583

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

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

Correct Answer: A

<https://itexamcertified.com>



- Expert Verified, Online, **Free**.

Custom View Settings

Question #1

Topic 1

A firm is developing a web application on AWS utilizing containers. At any one moment, the organization needs three instances of the web application to be running. The application must be scalable in order to keep up with demand increases. While management is cost-conscious, they agree that the application should be highly accessible.

What recommendations should a solutions architect make?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:/* as the action and Service:events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Correct Answer: C

Question #2

Topic 1

A firm seeks to migrate its accounting system from an on-premises data center to an Amazon Web Services (AWS) Region. Data security and an unalterable audit log should be prioritized. All AWS activities must be subjected to compliance audits. Despite the fact that the business has enabled AWS CloudTrail, it wants to guarantee that it meets these requirements.

What precautions and security procedures should a solutions architect include to protect and secure CloudTrail? (Choose two.)

- A. Create a second S3 bucket in us-east-1. Enable S3 Cross-Region Replication from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle management rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1 to store the replicated photos. Configure S3 event notifications on object creation and update events that invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: B

Question #3

Topic 1

A meteorological start-up company has created a custom web application for the aim of selling weather data to its members online. The company currently uses Amazon DynamoDB to store its data and wishes to establish a new service that alerts the managers of four internal teams whenever a new weather event is recorded. The business does not want for this new service to impair the operation of the present application.

What steps should a solutions architect take to guarantee that these objectives are satisfied with the MINIMUM feasible operational overhead?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary Index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A 

Question #4

Topic 1

A corporation uses an AWS application to offer content to its subscribers worldwide. Numerous Amazon EC2 instances are deployed on a private subnet behind an Application Load Balancer for the application (ALB). The chief information officer (CIO) wishes to limit access to some nations due to a recent change in copyright regulations.

Which course of action will satisfy these criteria?

- A. Modify the ALB security group to deny incoming traffic from blocked countries.
- B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.
- C. Use Amazon CloudFront to serve the application and deny access to blocked countries.
- D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

Correct Answer: C 

"block access for certain countries." You can use geo restriction, also known as geo blocking, to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

Question #5

Topic 1

Prior to delivering a new workload, a solutions architect must examine and update the organization's current IAM rules. The following policy was written by the solutions architect:

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Deny",  
    "NotAction": "s3:PutObject",  
    "Resource": "*",  
    "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": "false"}}  
  }]  
}
```

praw719528

What is the policy's net effect?

- A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.
- C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.
- D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

Correct Answer: D 

Question #6

Topic 1

Using seven Amazon EC2 instances, a business runs its web application on AWS. The organization needs that DNS queries provide the IP addresses of all healthy EC2 instances.

Which policy should be employed to comply with this stipulation?

- A. Simple routing policy
- B. Latency routing policy
- C. Multi-value routing policy
- D. Geolocation routing policy

Correct Answer: C 

Question #7

Topic 1

A business uses an Amazon RDS for PostgreSQL database instance to manage a fleet of web servers. Following a normal compliance review, the corporation establishes a standard requiring all production databases to have a recovery point objective (RPO) of less than one second.

Which solution satisfies these criteria?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Correct Answer: D 

Reference:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

Question #8

Topic 1

On Amazon EC2 instances, a business is developing an application that creates transitory transactional data. Access to data storage that can deliver adjustable and consistent IOPS is required by the application.

What recommendations should a solutions architect make?

- A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.
- B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.
- C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.
- D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

Correct Answer: C 

Question #9

Topic 1

To allow near-real-time processing, a web application must persist order data to Amazon S3. A solutions architect must design a scalable and fault-tolerant architecture.

Which solutions satisfy these criteria? (Select two.)

- A. Write the order event to an Amazon DynamoDB table. Use DynamoDB Streams to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- B. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use the queue to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- C. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use the SNS topic to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- D. Write the order event to an Amazon Simple Queue Service (Amazon SQS) queue. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.
- E. Write the order event to an Amazon Simple Notification Service (Amazon SNS) topic. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an AWS Lambda function that parses the payload and writes the data to Amazon S3.

Correct Answer: BE

Topic 1

A business is creating a website that will store static photos in an Amazon S3 bucket. The company's goal is to reduce both latency and cost for all future requests.

How should a solutions architect propose a service configuration?

- A. Deploy a NAT server in front of Amazon S3.
- B. Deploy Amazon CloudFront in front of Amazon S3.
- C. Deploy a Network Load Balancer in front of Amazon S3.
- D. Configure Auto Scaling to automatically adjust the capacity of the website.

Correct Answer: B

Reference:

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

Question #11

Topic 1

For the database layer of its ecommerce website, a firm uses Amazon DynamoDB with provided throughput. During flash sales, clients may encounter periods of delay when the database is unable to manage the volume of transactions. As a result, the business loses transactions. The database operates normally during regular times.

Which approach resolves the company's performance issue?

- A. Switch DynamoDB to on-demand mode during flash sales.
- B. Implement DynamoDB Accelerator for fast in memory performance.
- C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.
- D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

Correct Answer: A 

Question #12

Topic 1

In the AWS Cloud, a web application is deployed. It is a two-tier design comprised of a web and database layer. Cross-site scripting (XSS) attacks are possible on the web server.

What is the best course of action for a solutions architect to take to address the vulnerability?

- A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.
- D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

Correct Answer: C 

Working with cross-site scripting match conditions

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF Classic to inspect for possible malicious scripts. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious scripts.

Web Application Firewall -

You can now use AWS WAF to protect your web applications on your Application Load Balancers. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Reference:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

<https://aws.amazon.com/elasticloadbalancing/features/>

Question #13**Topic 1**

On its website, a business keeps a searchable store of things. The data is stored in a table with over ten million rows in an Amazon RDS for MySQL database. The database is stored on a 2 TB General Purpose SSD (gp2) array. Every day, the company's website receives millions of changes to this data. The organization found that certain activities were taking ten seconds or more and concluded that the bottleneck was the database storage performance.

Which option satisfies the performance requirement?

- A. Change the storage type to Provisioned IOPS SSD (io1).
- B. Change the instance to a memory-optimized instance class.
- C. Change the instance to a burstable performance DB instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Correct Answer: A **Question #14****Topic 1**

A business must give secure access to secret and sensitive data to its workers. The firm want to guarantee that only authorized individuals have access to the data. The data must be safely downloaded to workers' devices.

The files are kept on a Windows file server on-premises. However, as remote traffic increases, the file server's capacity is being depleted.

Which solution will satisfy these criteria?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

Correct Answer: C **Question #15****Topic 1**

A business is prepared to use Amazon S3 to store sensitive data. Data must be encrypted at rest for compliance purposes. Auditing of encryption key use is required. Each year, keys must be rotated.

Which solution satisfies these parameters and is the MOST OPTIMAL in terms of operational efficiency?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
- D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

Correct Answer: D 

Question #16

Topic 1

Management need a summary of AWS billed items broken down by user as part of their budget planning process. Budgets for departments will be created using the data. A solutions architect must ascertain the most effective method of obtaining this report data.

Which solution satisfies these criteria?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B 

Question #17

Topic 1

A legal company must communicate with the public. Hundreds of files must be publicly accessible. Anyone is banned from modifying or deleting the files before to a specified future date.

Which solution satisfies these criteria the SAFEST way possible?

- A. Upload all flies to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.
- B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
- C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
- D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Correct Answer: D 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html>

Question #18

Topic 1

A corporation connects its on-premises servers to AWS through a 10 Gbps AWS Direct Connect connection. The connection's workloads are crucial. The organization needs a catastrophe recovery approach that is as resilient as possible while minimizing the existing connection bandwidth.

What recommendations should a solutions architect make?

- A. Set up a new Direct Connect connection in another AWS Region.
- B. Set up a new AWS managed VPN connection in another AWS Region.
- C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.
- D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

Correct Answer: C 

Question #19

Topic 1

A business has two virtual private clouds (VPCs) labeled Management and Production. The Management VPC connects to a single device in the data center using VPNs via a customer gateway. The Production VPC is connected to AWS through two AWS Direct Connect connections via a virtual private gateway. Both the Management and Production VPCs communicate with one another through a single VPC peering connection.

What should a solutions architect do to minimize the architecture's single point of failure?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: A 

Question #20

Topic 1

Currently, a company's legacy application relies on an unencrypted single-instance Amazon RDS MySQL database. All current and new data in this database must be encrypted to comply with new compliance standards.

How is this to be achieved?

- A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.
- B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.
- C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.
- D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance.

Correct Answer: C 

How do I encrypt Amazon RDS snapshots?

The following steps are applicable to Amazon RDS for MySQL, Oracle, SQL Server, PostgreSQL, or MariaDB.

Important: If you use Amazon Aurora, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster if you specify an AWS Key

Management Service (AWS KMS) encryption key when you restore from the unencrypted DB cluster snapshot. For more information, see

Limitations of Amazon

RDS Encrypted DB Instances.

Open the Amazon RDS console, and then choose Snapshots from the navigation pane.

Select the snapshot that you want to encrypt.

Under Snapshot Actions, choose Copy Snapshot.

Choose your Destination Region, and then enter your New DB Snapshot Identifier.

Change Enable Encryption to Yes.

Select your Master Key from the list, and then choose Copy Snapshot.

After the snapshot status is available, the Encrypted field will be True to indicate that the snapshot is encrypted.

You now have an encrypted snapshot of your DB. You can use this encrypted DB snapshot to restore the DB instance from the DB snapshot.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/encrypt-rds-snapshots/>

Question #21

Topic 1

A company's website stores transactional data on an Amazon RDS MySQL Multi-AZ DB instance. Other internal systems query this database instance to get data for batch processing. When internal systems request data from the RDS DB instance, the RDS DB instance drastically slows down. This has an adverse effect on the website's read and write performance, resulting in poor response times for users.

Which approach will result in an increase in website performance?

- A. Use an RDS PostgreSQL DB instance instead of a MySQL database.
- B. Use Amazon ElastiCache to cache the query responses for the website.
- C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.
- D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

Correct Answer: D 

Amazon RDS Read Replicas -

Enhanced performance -

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Because read replicas can be promoted to master status, they are useful as part of a sharding implementation.

To further maximize read performance, Amazon RDS for MySQL allows you to add table indexes directly to Read Replicas, without those indexes being present on the master.

Reference:

<https://aws.amazon.com/rds/features/read-replicas>

Question #22

Topic 1

AWS hosts a company's near-real-time streaming application. While the data is being ingested, a job is being performed on it that takes 30 minutes to finish. Due to the massive volume of incoming data, the workload regularly faces significant latency. To optimize performance, a solutions architect must build a scalable and serverless system.

Which actions should the solutions architect do in combination? (Select two.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Correct Answer: AE 

Question #23

Topic 1

Amazon Elastic Block Store (Amazon EBS) volumes are used by a media organization to store video material. A certain video file has gained popularity, and a significant number of individuals from all over the globe are now viewing it. As a consequence, costs have increased.

Which step will result in a cost reduction without jeopardizing user accessibility?

- A. Change the EBS volume to Provisioned IOPS (PIOPS).
- B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.
- C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.
- D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

Correct Answer: B 

Question #24

Topic 1

Amazon S3 buckets are used by an image hosting firm to store its objects. The firm wishes to prevent unintentional public disclosure of the items contained in the S3 buckets. All S3 items in the AWS account as a whole must remain private.

Which solution will satisfy these criteria?

- A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
- B. Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.
- C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
- D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-ug.pdf>

Question #25

Topic 1

A marketing firm uses an Amazon S3 bucket to store CSV data for statistical research. Permission is required for an application running on an Amazon EC2 instance to properly handle the CSV data stored in the S3 bucket.

Which step will provide the MOST SECURE access to the S3 bucket for the EC2 instance?

- A. Attach a resource-based policy to the S3 bucket.
- B. Create an IAM user for the application with specific permissions to the S3 bucket.
- C. Associate an IAM role with least privilege permissions to the EC2 instance profile.
- D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

Correct Answer: C 

Question #26

Topic 1

On a cluster of Amazon Linux EC2 instances, a business runs an application. The organization is required to store all application log files for seven years for compliance purposes.

The log files will be evaluated by a reporting program, which will need concurrent access to all files.

Which storage system best satisfies these criteria in terms of cost-effectiveness?

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

Correct Answer: D 

Amazon S3 -

Requests to Amazon S3 can be authenticated or anonymous. Authenticated access requires credentials that AWS can use to authenticate your requests. When making REST API calls directly from your code, you create a signature using valid credentials and include the signature in your request. Amazon Simple Storage

Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Reference:

<https://aws.amazon.com/s3/>

Question #27

Topic 1

On a fleet of Amazon EC2 instances, a business provides a training site. The business predicts that when its new course, which includes hundreds of training videos on the web, is available in one week, it will be tremendously popular.

What should a solutions architect do to ensure that the predicted server load is kept to a minimum?

- A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.
- B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.
- C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.
- D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

Correct Answer: C 

Question #28

Topic 1

A business chooses to transition from on-premises to the AWS Cloud its three-tier web application. The new database must be able to scale storage capacity dynamically and conduct table joins.

Which AWS service satisfies these criteria?

- A. Amazon Aurora
- B. Amazon RDS for SqlServer
- C. Amazon DynamoDB Streams
- D. Amazon DynamoDB on-demand

Correct Answer: A 

Question #29

Topic 1

On a fleet of Amazon EC2 instances, a business runs a production application. The program takes data from an Amazon SQS queue and concurrently processes the messages. The message volume is variable, and traffic is often interrupted. This program should handle messages continuously and without interruption.

Which option best fits these criteria in terms of cost-effectiveness?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Correct Answer: C 

Question #30

Topic 1

A business requires data storage on Amazon S3. A compliance requirement stipulates that when objects are modified, their original state must be retained. Additionally, data older than five years should be kept for auditing purposes.

What SHOULD A SOLUTIONS ARCHITECT RECOMMEND AS THE MOST EFFORTABLE?

- A. Enable object-level versioning and S3 Object Lock in governance mode
- B. Enable object-level versioning and S3 Object Lock in compliance mode
- C. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive
- D. Enable object-level versioning. Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

Correct Answer: C 

Question #31

Topic 1

Multiple Amazon EC2 instances are used to host an application. The program reads messages from an Amazon SQS queue, writes them to an Amazon RDS database, and then removes them from the queue. The RDS table sometimes contains duplicate entries. There are no duplicate messages in the SQS queue.

How can a solutions architect guarantee that messages are handled just once?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Correct Answer: D 

Question #32

Topic 1

A corporation just announced the worldwide launch of their retail website. The website is hosted on numerous Amazon EC2 instances, which are routed via an Elastic Load Balancer. The instances are distributed across several Availability Zones in an Auto Scaling group.

The firm want to give its clients with customized material depending on the device from which they view the website.

Which steps should a solutions architect perform in combination to satisfy these requirements? (Select two.)

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Correct Answer: CE 

Question #33

Topic 1

A newly formed company developed a three-tiered web application. The front end is comprised entirely of static information. Microservices form the application layer. User data is kept in the form of JSON documents that must be accessible with a minimum of delay. The firm anticipates minimal regular traffic in the first year, with monthly traffic spikes. The startup team's operational overhead expenditures must be kept to a minimum.

What should a solutions architect suggest as a means of achieving this?

- A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.
- B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.
- C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.
- D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

Correct Answer: C 

Question #34

Topic 1

To facilitate experimentation and agility, a business enables developers to link current IAM policies to existing IAM roles. The security operations team, on the other hand, is worried that the developers may attach the current administrator policy, allowing them to bypass any other security rules.

What approach should a solutions architect use in dealing with this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM activity across all account in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Correct Answer: D 

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Question #35

Topic 1

Amazon Elastic Container Service (Amazon ECS) container instances are used to install an ecommerce website's web application behind an Application Load Balancer (ALB). The website slows down and availability is decreased during moments of heavy usage. A solutions architect utilizes Amazon CloudWatch alarms to be notified when an availability problem occurs, allowing them to scale out resources. The management of the business want a system that automatically reacts to such circumstances.

Which solution satisfies these criteria?

- A. Set up AWS Auto Scaling to scale out the ECS service when there are timeouts on the ALB. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- B. Set up AWS Auto Scaling to scale out the ECS service when the ALB CPU utilization is too high. Setup AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- C. Set up AWS Auto Scaling to scale out the ECS service when the service's CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.
- D. Set up AWS Auto Scaling to scale out the ECS service when the ALB target group CPU utilization is too high. Set up AWS Auto Scaling to scale out the ECS cluster when the CPU or memory reservation is too high.

Correct Answer: A 

Question #36

Topic 1

A business uses Site-to-Site VPN connections to provide safe access to AWS Cloud services from on-premises. Users are experiencing slower VPN connectivity as a result of increased traffic through the VPN connections to the Amazon EC2 instances.

Which approach will result in an increase in VPN throughput?

- A. Implement multiple customer gateways for the same network to scale the throughput.
- B. Use a transit gateway with equal cost multipath routing and add additional VPN tunnels.
- C. Configure a virtual private gateway with equal cost multipath routing and multiple channels.
- D. Increase the number of tunnels in the VPN configuration to scale the throughput beyond the default limit.

Correct Answer: A 

Question #37

Topic 1

On Amazon EC2 Linux instances, a business hosts a website. Several of the examples are malfunctioning. The troubleshooting indicates that the unsuccessful instances lack swap space. The operations team's lead need a monitoring solution for this.

What recommendations should a solutions architect make?

- A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
- B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
- C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
- D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

Question #38

Topic 1

AWS is used by a business to perform an online transaction processing (OLTP) burden. This workload is deployed in a Multi-AZ environment using an unencrypted Amazon RDS database instance. This instance's database is backed up daily.

What should a solutions architect do going forward to guarantee that the database and snapshots are constantly encrypted?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Correct Answer: A 

Question #39

Topic 1

A business operates an application that collects data from its consumers through various Amazon EC2 instances. After processing, the data is uploaded to Amazon S3 for long-term storage. A study of the application reveals that the EC2 instances were inactive for extended periods of time. A solutions architect must provide a system that maximizes usage while minimizing expenditures.

Which solution satisfies these criteria?

- A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.
- B. Build the application to use Amazon Lightsail with On-Demand Instances.
- C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.
- D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

Correct Answer: D 

Question #40

Topic 1

A solutions architect is developing a daily data processing task that will take up to two hours to finish. If the task is stopped, it must be restarted from scratch.

What is the MOST cost-effective way for the solutions architect to solve this issue?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

Correct Answer: C 

Question #41

Topic 1

A business intends to use AWS to host a survey website. The firm anticipated a high volume of traffic. As a consequence of this traffic, the database is updated asynchronously. The organization want to avoid dropping writes to the database housed on AWS.

How should the business's application be written to handle these database requests?

- A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.
- B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

Correct Answer: A 

Question #42

Topic 1

On a huge fleet of Amazon EC2 instances, a business runs an application. The program reads and writes items to a DynamoDB database hosted by Amazon. The DynamoDB database increases in size regularly, yet the application requires just data from the previous 30 days. The organization need a solution that is both cost effective and time efficient to implement.

Which solution satisfies these criteria?

- A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
- B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
- C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
- D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Correct Answer: D 

Question #43

Topic 1

Previously, a corporation moved their data warehousing solution to AWS. Additionally, the firm has an AWS Direct Connect connection. Through the use of a visualization tool, users in the corporate office may query the data warehouse. Each query answered by the data warehouse is on average 50 MB in size, whereas each webpage supplied by the visualization tool is around 500 KB in size. The data warehouse does not cache the result sets it returns.

Which approach results in the LOWEST OUTGOING DATA TRANSFER COSTS FOR THE COMPANY?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in the same Region.

Correct Answer: A 

Question #44

Topic 1

A business is developing an application that is composed of many microservices. The organization has chosen to deploy its software on AWS through container technology. The business need a solution that requires little ongoing work for maintenance and growth. Additional infrastructure cannot be managed by the business.

Which steps should a solutions architect perform in combination to satisfy these requirements? (Select two.)

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Correct Answer: AB 

Question #45

Topic 1

The following policy was developed by an Amazon EC2 administrator and assigned to an IAM group including numerous users:

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

What impact does this policy have?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Correct Answer: C 

Question #46

Topic 1

A solutions architect is developing a hybrid application on the Amazon Web Services (AWS) cloud. AWS Direct Link (DX) will be used to connect the on-premises data center to AWS. Between AWS and the on-premises data center, the application connection must be very durable.

Which DX setup should be used to satisfy these criteria?

- A. Configure a DX connection with a VPN on top of it.
- B. Configure DX connections at multiple DX locations.
- C. Configure a DX connection using the most reliable DX partner.
- D. Configure multiple virtual interfaces on top of a DX connection.

Correct Answer: B 

Question #47

Topic 1

The web application of a business stores its data on an Amazon RDS PostgreSQL database instance. Accountants conduct massive queries at the start of each month during the financial closure period, which has a negative influence on the database's performance owing to excessive utilization. The business want to reduce the effect of reporting on the online application.

What should a solutions architect do to minimize the database's influence with the LEAST amount of work possible?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Correct Answer: A 

Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines' built-in replication functionality to create a special type of

DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections. Applications connect to a read replica the same way they do to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #48

Topic 1

A financial institution uses AWS to host a web application. The program retrieves current stock prices using an Amazon API Gateway Regional API endpoint. The security staff at the organization has detected an upsurge in API queries. The security team is worried that HTTP flood attacks may result in the application being rendered inoperable.

A solutions architect must create a defense against this form of assault.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Correct Answer: C 

Question #49

Topic 1

A business wishes to automate the evaluation of the security of its Amazon EC2 instances. The organization must verify and show that the development process adheres to security and compliance requirements.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.
- B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.
- C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications
- D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

Correct Answer: C 

Question #50

Topic 1

On Amazon EC2, a corporation is operating a highly secure application that is backed up by an Amazon RDS database. All personally identifiable information (PII) must be encrypted at rest to comply with compliance standards.

Which solution should a solutions architect propose in order to achieve this need with the MINIMUM number of infrastructure changes?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

Correct Answer: D 

Question #51

Topic 1

The following IAM policy has been established by a solutions architect.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "lambda:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": [  
                "lambda:CreateFunction",  
                "lambda>DeleteFunction"  
            ],  
            "Resource": "*"  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "220.100.16.0/20"  
                }  
            }  
        }  
    ]  
}
```

praw709528

Which actions will the policy permit?

- A. An AWS Lambda function can be deleted from any network.
- B. An AWS Lambda function can be created from any network.
- C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.
- D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

Correct Answer: C 

Question #52

Topic 1

On Amazon Aurora, a business is operating a database. Every nightfall, the database is inactive. When user traffic surges in the early hours, an application that makes large reads on the database will face performance concerns. When reading from the database during these peak hours, the program encounters timeout issues. Due to the lack of a dedicated operations crew, the organization need an automated solution to solve performance concerns.

Which activities should a solutions architect take to ensure that the database automatically adjusts to the increasing read load? (Select two.)

- A. Migrate the database to Aurora Serverless.
- B. Increase the instance size of the Aurora database.
- C. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Migrate the database to an Aurora multi-master cluster.
- E. Migrate the database to an Amazon RDS for MySQL Multi-AZ deployment.

Correct Answer: CD 

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Performance.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-multi-master.html>

Question #53**Topic 1**

An Amazon EC2 instance-based application requires access to an Amazon DynamoDB database. The EC2 instance and DynamoDB table are both managed by the same AWS account. Permissions must be configured by a solutions architect.

Which approach will provide the EC2 instance least privilege access to the DynamoDB table?

- A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.
- B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.
- C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.
- D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

Correct Answer: A **Question #54****Topic 1**

Users may get past performance reports from a company's website. The website requires a solution that can grow to suit the company's worldwide website requirements. The solution should be cost-effective, minimize infrastructure resource provisioning, and deliver the quickest reaction time feasible.

Which mix of technologies might a solutions architect propose in order to satisfy these requirements?

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A **Question #55****Topic 1**

A business uses Amazon EC2 instances to operate an API-based inventory reporting application. The program makes use of an Amazon DynamoDB database to store data. The distribution centers of the corporation use an on-premises shipping application that communicates with an API to update inventory prior to generating shipping labels. Each day, the organization has seen application outages, resulting in missed transactions.

What should a solutions architect propose to increase the resilience of an application?

- A. Modify the shipping application to write to a local database.
- B. Modify the application APIs to run serverless using AWS Lambda
- C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
- D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

Correct Answer: A 

Question #56*Topic 1*

Amazon EC2 instances on private subnets are used to execute an application. The application requires access to a table in Amazon DynamoDB.

What is the MOST SECURE method of accessing the table without allowing traffic to exit the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Correct Answer: A **Question #57***Topic 1*

On a single Amazon EC2 instance, a business runs an ASP.NET MVC application. Due to a recent spike in application usage, users are experiencing poor response times during lunch hours. The firm must address this issue using the least amount of settings possible.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours.
- B. Move the application to Amazon Elastic Container Service (Amazon ECS). Create an AWS Lambda function to handle scaling during lunch hours.
- C. Move the application to Amazon Elastic Container Service (Amazon ECS). Configure scheduled scaling for AWS Application Auto Scaling during lunch hours.
- D. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling, and create an AWS Lambda function to handle scaling during lunch hours.

Correct Answer: A **Reference:**

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-autoscaling-scheduledactions.html>

Question #58

Topic 1

Amazon Redshift is being used by a business to do analytics and produce customer reports. The corporation just obtained an extra 50 terabytes of demographic data on its customers. The data is saved in Amazon S3 in.csv files. The organization need a system that efficiently merges data and visualizes the findings.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Use Amazon Redshift Spectrum to query the data in Amazon S3 directly and join that data with the existing data in Amazon Redshift. Use Amazon QuickSight to build the visualizations.
- B. Use Amazon Athena to query the data in Amazon S3. Use Amazon QuickSight to join the data from Athena with the existing data in Amazon Redshift and to build the visualizations.
- C. Increase the size of the Amazon Redshift cluster, and load the data from Amazon S3. Use Amazon EMR Notebooks to query the data and build the visualizations in Amazon Redshift.
- D. Export the data from the Amazon Redshift cluster into Apache Parquet files in Amazon S3. Use Amazon Elasticsearch Service (Amazon ES) to query the data. Use Kibana to visualize the results.

Correct Answer: A 

Question #59

Topic 1

Each month, a business keeps 200 GB of data on Amazon S3. At the conclusion of each month, the corporation must analyze this data to calculate the number of things sold in each sales area during the preceding month.

Which analytics approach is the MOST cost-effective option for the business?

- A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.
- B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.
- C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.
- D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

Correct Answer: A 

Question #60

Topic 1

A business is in the process of migrating its on-premises application to AWS. Program servers and a Microsoft SQL Server database comprise the application. The database cannot be transferred to another engine due to the application's .NET code using SQL Server functionality. The company's goal is to maximize availability while decreasing operational and administration costs.

What actions should a solutions architect take to achieve this?

- A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.
- B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.
- C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.
- D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

Correct Answer: B 

Question #61

Topic 1

A business's data layer is powered by Amazon RDS for PostgreSQL databases. The organization must adopt database password rotation.

Which option satisfies this criterion with the LEAST amount of operational overhead?

- A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.
- B. Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.
- C. Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.
- D. Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the customer master key (CMK).

Correct Answer: A 

Reference -

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

Question #62

Topic 1

Within the same AWS account, a firm has two VPCs situated in the us-west-2 Region. The business must permit network communication between these VPCs. Each month, about 500 GB of data will be transferred between the VPCs.

Which approach is the MOST cost-effective for connecting these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Correct Answer: D 

Question #63

Topic 1

A business's production workload is hosted on an Amazon Aurora MySQL DB cluster comprised of six Aurora Replicas. The corporation wishes to automate the distribution of near-real-time reporting requests from one of its departments among three Aurora Replicas. These three copies are configured differently from the rest of the DB cluster in terms of computation and memory.

Which solution satisfies these criteria?

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

Correct Answer: B 

Question #64

Topic 1

A business's on-premises data center has reached its storage limit. The organization wishes to shift its storage system to AWS while keeping bandwidth costs as low as possible. The solution must enable rapid and cost-free data retrieval.

How are these stipulations to be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
- C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
- D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

Correct Answer: B 

Question #65

Topic 1

Within a month of being bought, a newly acquired firm is needed to establish its own infrastructure on AWS and transfer various apps to the cloud. Each application requires the transmission of around 50 TB of data. Following the transfer, this firm and its parent company will need secure network connection with constant throughput between its data centers and apps. A solutions architect must guarantee that data transfer occurs just once and that network connection is maintained.

Which solution will satisfy these criteria?

- A. AWS Direct Connect for both the initial transfer and ongoing connectivity.
- B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
- C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.
- D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

Correct Answer: C 

Reference:

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html <https://aws.amazon.com/directconnect/>

Question #66

Topic 1

A solutions architect must create a solution that retrieves data every two minutes from an internet-based third-party web service. Each data retrieval is performed using a Python script in less than 100 milliseconds. The answer is a JSON object of less than 1 KB in size including sensor data. The architect of the solution must keep both the JSON object and the date.

Which approach is the most cost-effective in meeting these requirements?

- A. Deploy an Amazon EC2 instance with a Linux operating system. Configure a cron job to run the script every 2 minutes. Extend the script to store the JSON object along with the timestamp in a MySQL database that is hosted on an Amazon RDS DB instance.
- B. Deploy an Amazon EC2 instance with a Linux operating system to extend the script to run in an infinite loop every 2 minutes. Store the JSON object along with the timestamp in an Amazon DynamoDB table that uses the timestamp as the primary key. Run the script on the EC2 instance.
- C. Deploy an AWS Lambda function to extend the script to store the JSON object along with the timestamp in an Amazon DynamoDB table that uses the timestamp as the primary key. Use an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that is initiated every 2 minutes to invoke the Lambda function.
- D. Deploy an AWS Lambda function to extend the script to run in an infinite loop every 2 minutes. Store the JSON object along with the timestamp in an Amazon DynamoDB table that uses the timestamp as the primary key. Ensure that the script is called by the handler function that is configured for the Lambda function.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/connect/latest/adminguide/connect-ag.pdf>

Question #67

Topic 1

A business intends to transfer a TCP-based application onto the company's virtual private cloud (VPC). The program is available to the public over an unsupported TCP port via a physical device located in the company's data center. This public endpoint has a latency of less than 3 milliseconds and can handle up to 3 million requests per second. The organization needs the new public endpoint in AWS to function at the same level of performance.

What solution architecture approach should be recommended to satisfy this requirement?

- A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.
- B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.
- C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.
- D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

Correct Answer: C 

Question #68

Topic 1

A business does not currently have any file sharing services. A new project needs file storage that can be mounted as a disk for on-premises desktop computers. Before users can access the storage, the file server must authenticate them against an Active Directory domain.

Which service enables Active Directory users to deploy storage on their workstations as a drive?

- A. Amazon S3 Glacier
- B. AWS DataSync
- C. AWS Snowball Edge
- D. AWS Storage Gateway

Correct Answer: D 

Question #69

Topic 1

A corporation with an on-premises application is transitioning to AWS to boost the flexibility and availability of the application. The present design makes considerable use of a Microsoft SQL Server database. The firm want to investigate other database solutions and, if necessary, migrate database engines.

The development team does a complete copy of the production database every four hours in order to create a test database. Users will encounter delay during this time period.

What database should a solution architect propose as a replacement?

- A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.
- B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.
- D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

Correct Answer: D 

Question #70

Topic 1

On Amazon EC2 instances, a business runs an application. The volume of traffic to the webpage grows significantly during business hours and then falls.

The CPU usage of an Amazon EC2 instance is a good measure of the application's end-user demand. The organization has specified a minimum group size of two EC2 instances and a maximum group size of ten EC2 instances for an Auto Scaling group.

The firm is worried that the Auto Scaling group's existing scaling policy may be incorrect. The organization must prevent excessive EC2 instance provisioning and paying unneeded fees.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.
- B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.
- C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.
- D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

Correct Answer: D 

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

Question #71

Topic 1

A company's on-premises infrastructure and AWS need a secure connection. This connection does not need a large quantity of bandwidth and is capable of handling a limited amount of traffic. The link should be established immediately.

Which way is the MOST CHEAPEST for establishing this sort of connection?

- A. Implement a client VPN.
- B. Implement AWS Direct Connect.
- C. Implement a bastion host on Amazon EC2.
- D. Implement an AWS Site-to-Site VPN connection.

Correct Answer: D 

Question #72

Topic 1

A business is developing a web-based application that will operate on Amazon EC2 instances distributed across several Availability Zones. The online application will enable access to a collection of over 900 TB of text content. The corporation expects times of heavy demand for the online application. A solutions architect must guarantee that the text document storage component can scale to meet the application's demand at all times. The corporation is concerned about the solution's total cost.

Which storage system best satisfies these criteria in terms of cost-effectiveness?

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

Correct Answer: C 

Reference:

<https://www.missioncloud.com/blog/resource-amazon-ebs-vs-efs-vs-s3-picking-the-best-aws-storage-option-for-your-business>

Question #73

Topic 1

A business is using a tape backup system to offshore store critical application data. Daily data volume is in the neighborhood of 50 TB. For regulatory requirements, the firm must maintain backups for seven years. Backups are infrequently viewed, and a week's notice is normally required before restoring a backup.

The organization is now investigating a cloud-based solution in order to cut storage expenses and the operational load associated with tape management. Additionally, the organization wants to ensure that the move from tape backups to the cloud is as seamless as possible.

Which storage option is the CHEAPEST?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

Correct Answer: A 

Question #74*Topic 1*

A business has launched a mobile multiplayer game. The game demands real-time monitoring of participants' latitude and longitude positions. The game's data storage must be capable of quick updates and location retrieval. The game stores location data on an Amazon RDS for PostgreSQL DB instance with read replicas. The database is unable to sustain the speed required for reading and writing changes during high use times. The game's user base is rapidly growing.

What should a solutions architect do to optimize the data tier's performance?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

Correct Answer: C **Question #75***Topic 1*

A development team must have a website that is accessible to other development teams. HTML, CSS, client-side JavaScript, and graphics comprise the website's content.

Which form of website hosting is the MOST cost-effective?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Correct Answer: B **Question #76***Topic 1*

A business's data warehouse is powered by Amazon Redshift. The firm want to assure the long-term viability of its data in the event of component failure.

What recommendations should a solutions architect make?

- A. Enable concurrency scaling.
- B. Enable cross-Region snapshots.
- C. Increase the data retention period.
- D. Deploy Amazon Redshift in Multi-AZ.

Correct Answer: B 

Question #77

Topic 1

A business offers its customers with an API that automates tax calculations based on item pricing. During the Christmas season, the firm receives an increased volume of queries, resulting in delayed response times. A solutions architect must create a scalable and elastic system.

What is the solution architect's role in achieving this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Correct Answer: B 

Question #78

Topic 1

A solutions architect is designing a VPC architecture with various subnets. Six subnets will be used in two Availability Zones. Subnets are classified as public, private, and database-specific. Access to a database should be restricted to Amazon EC2 instances operating on private subnets.

Which solution satisfies these criteria?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
- B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
- C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Correct Answer: B 

Question #79

Topic 1

A business is implementing a web gateway. The firm want to limit public access to the program to the online part. The VPC was created with two public subnets and two private subnets to achieve this. The application will be hosted on many Amazon EC2 instances that will be managed through an Auto Scaling group. SSL termination must be delegated to a separate instance on Amazon EC2.

What actions should a solutions architect take to guarantee compliance with these requirements?

- A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.
- C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.
- D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

Correct Answer: C 

Question #80

Topic 1

A business uses the SMB protocol to back up on-premises databases to local file server shares. To accomplish recovery goals, the organization needs instant access to one week's worth of backup data. After a week, recovery is less possible, and the business may live with a delay in retrieving those earlier backup data.

What actions should a solutions architect take to ensure that these criteria are met with the LEAST amount of operational work possible?

- A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.
- B. Deploy an AWS Storage Gateway file gateway with sufficient storage to hold 1 week of backups. Point the backups to SMB shares from the file gateway.
- C. Deploy Amazon Elastic File System (Amazon EFS) to create a file system with exposed NFS shares with sufficient storage to hold all the desired backups.
- D. Continue to back up to the existing file shares. Deploy AWS Database Migration Service (AWS DMS) and define a copy task to copy backup files older than 1 week to Amazon S3, and delete the backup files from the local file store.

Correct Answer: A 

Question #81

Topic 1

A business is operating a worldwide application. Users upload various videos, which are subsequently combined into a single video file. The program receives uploads from users through a single Amazon S3 bucket in the us-east-1 Region. The same S3 bucket also serves as the download point for the generated video file. The finished video file is around 250 GB in size.

The organization requires a solution that enables quicker uploads and downloads of video files stored in Amazon S3. The corporation will charge consumers who choose to pay for the faster speed a monthly fee.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Enable AWS Global Accelerator for the S3 endpoint. Adjust the application's upload and download links to use the Global Accelerator S3 endpoint for users who have a subscription.
- B. Enable S3 Cross-Region Replication to S3 buckets in all other AWS Regions. Use an Amazon Route 53 geolocation routing policy to route S3 requests based on the location of users who have a subscription.
- C. Create an Amazon CloudFront distribution and use the S3 bucket in us-east-1 as an origin. Adjust the application to use the CloudFront URL as the upload and download links for users who have a subscription.
- D. Enable S3 Transfer Acceleration for the S3 bucket in us-east-1. Configure the application to use the bucket's S3-accelerate endpoint domain name for the upload and download links for users who have a subscription.

Correct Answer: C 

Question #82

Topic 1

A daily scheduled task must be executed by an ecommerce business to collect and filter sales statistics for analytics purposes. The sales records are stored in an Amazon S3 bucket. Each object has a maximum file size of 10 GB. The work might take up to an hour to complete depending on the amount of sales events. The job's CPU and memory requirements are consistent and known in advance.

A solutions architect's goal is to reduce the amount of operational work required to complete the task.

Which solution satisfies these criteria?

- A. Create an AWS Lambda function that has an Amazon EventBridge (Amazon CloudWatch Events) notification. Schedule the EventBridge (CloudWatch Events) event to run once a day.
- B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API. and integrate the API with the function. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that calls the API and invokes the function.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that launches an ECS task on the cluster to run the job.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that launches an ECS task on the cluster to run the job.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-run-lambda-schedule.html>

Question #83

Topic 1

A shopping cart application connects to an Amazon RDS Multi-AZ database instance. The database performance is causing the application to slow down. There was no significant performance improvement after upgrading to the next-generation instance type. According to the analysis, around 700 IOPS are maintained, typical queries execute for extended periods of time, and memory use is significant.

Which application modification might a solutions architect propose to address these concerns?

- A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
- B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
- C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
- D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

Correct Answer: C 

Question #84

Topic 1

A startup is developing a shared storage solution for an AWS Cloud-hosted gaming application. The organization need the capacity to access data through SMB clients. The solution must be controlled completely.

Which AWS solution satisfies these criteria?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- C. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

Correct Answer: C 

Reference:

<https://aws.amazon.com/fsx/windows/>

Question #85

Topic 1

A business relies on Amazon S3 for object storage. The organization stores data in hundreds of S3 buckets. Certain S3 buckets contain less frequently accessed data than others. According to a solutions architect, lifecycle rules are either not followed consistently or are enforced in part, resulting in data being held in high-cost storage.

Which option will reduce expenses without jeopardizing object availability?

- A. Use S3 ACLs.
- B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.
- C. Use S3 Intelligent-Tiering storage.
- D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C 

Question #86**Topic 1**

A business is re-architecting a tightly connected application in order to make it loosely coupled. Previously, the program communicated across layers through a request/response pattern. The organization intends to do this via the usage of Amazon Simple Queue Service (Amazon SQS). The first architecture includes a request queue and a response queue. However, when the program grows, this strategy will not handle all messages.

What is the best course of action for a solutions architect to take in order to tackle this issue?

- A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.
- B. Configure a FIFO queue, and use the message deduplication ID and message group ID.
- C. Create a temporary queue, with the Temporary Queue Client to receive each response message.
- D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

Correct Answer: A **Question #87****Topic 1**

Amazon S3 is used by a business to store private audit records. According to the concept of least privilege, the S3 bucket implements bucket restrictions to limit access to audit team IAM user credentials. Company executives are concerned about inadvertent document destruction in the S3 bucket and need a more secure solution.

What steps should a solutions architect take to ensure the security of audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html>**Question #88****Topic 1**

Application developers have found that when business reporting users run big production reports to the Amazon RDS instance that powers the application, the application becomes very sluggish. While the reporting queries are executing, the RDS instance's CPU and memory usage metrics do not surpass 60%.

Business reporting users must be able to produce reports without impairing the functionality of the application.

Which action is necessary to achieve this?

- A. Increase the size of the RDS instance.
- B. Create a read replica and connect the application to it.
- C. Enable multiple Availability Zones on the RDS instance.
- D. Create a read replica and connect the business reports to it.

Correct Answer: D 

Question #89

Topic 1

Each day, a company's hundreds of edge devices create 1 TB of status alerts. Each alert has a file size of roughly 2 KB. A solutions architect must provide a system for ingesting and storing warnings for further investigation. The business need a solution that is extremely accessible. However, the business must have a low cost structure and does not want to handle extra infrastructure. Additionally, the corporation intends to retain 14 days of data for instant examination and archive any older data.

What is the MOST OPTIMAL option that satisfies these requirements?

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

Correct Answer: A 

Question #90

Topic 1

A firm runs a two-tier image processing program. The application is divided into two Availability Zones, each with its own public and private subnets.

The web tier's Application Load Balancer (ALB) makes use of public subnets. Private subnets are used by Amazon EC2 instances at the application layer.

The program is functioning more slowly than planned, according to users. According to a security audit of the web server log files, the application receives millions of unauthorized requests from a tiny number of IP addresses. While the organization finds a more permanent solution, a solutions architect must tackle the urgent performance issue.

What solution architecture approach should be recommended to satisfy this requirement?

- A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
- B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
- C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
- D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Correct Answer: B 

Question #91

Topic 1

A business uses Amazon Elastic Container Service (Amazon ECS) to perform an image processing workload on two private subnets. Each private subnet connects to the internet through a NAT instance. Amazon S3 buckets are used to store all photos. The business is worried about the expenses associated with data transfers between Amazon ECS and Amazon S3.

What actions should a solutions architect do to save money?

- A. Configure a NAT gateway to replace the NAT instances.
- B. Configure a gateway endpoint for traffic destined to Amazon S3.
- C. Configure an interface endpoint for traffic destined to Amazon S3.
- D. Configure Amazon CloudFront for the S3 bucket storing the images.

Correct Answer: C 

Question #92

Topic 1

An online picture program enables users to upload photographs and modify them. The application provides two distinct service levels: free and paid. Paid users' photos are processed ahead of those submitted by free users. Amazon S3 is used to store the photos, while Amazon SQS is used to store the job information.

How should a solutions architect propose a configuration?

- A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.
- B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.
- C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.
- D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

Correct Answer: A 

Question #93

Topic 1

A new employee has been hired as a deployment engineer by a corporation. The deployment engineer will construct several AWS resources using AWS CloudFormation templates. A solutions architect desires that the deployment engineer execute job functions with the least amount of privilege possible.

Which steps should the solutions architect do in conjunction to reach this goal? (Select two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

Correct Answer: DE 

Question #94

Topic 1

A corporation is using AWS to construct a new machine learning model solution. The models are constructed as self-contained microservices that get around 1 GB of model data from Amazon S3 and put it into memory during startup. The models are accessed by users through an asynchronous API. Users may submit a single request or a batch of requests and designate the destination for the results.

Hundreds of people benefit from the company's models. The models' use habits are erratic. Certain models may go days or weeks without being used. Other models may get hundreds of queries concurrently.

Which solution satisfies these criteria?

- A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.
- B. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.
- C. The requests from the API are sent to the model's Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.
- D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

Correct Answer: D 

Question #95

Topic 1

Each month, a leasing firm prepares and delivers PDF statements to all of its clients. Each statement is around 400 KB in length. Customers may obtain their statements from the website for a period of up to 30 days after they are created. Customers are sent a ZIP file containing all of their statements at the conclusion of their three-year lease.

Which storage method is the MOST cost-effective in this situation?

- A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.
- B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.
- C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.
- D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

Correct Answer: B 

Question #96

Topic 1

A firm just launched a two-tier application in the us-east-1 Region's two Availability Zones. Databases are located on a private subnet, whereas web servers are located on a public subnet. The VPC is connected to the internet through an internet gateway. Amazon EC2 instances are used to host the application and database. The database servers are unable to connect to the internet in order to get fixes. A solutions architect must create a system that ensures database security while incurring the fewest operating costs.

Which solution satisfies these criteria?

- A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.
- C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.
- D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

Correct Answer: A 

Question #97

Topic 1

A company's ecommerce site is seeing a rise in visitor visits. The company's shop is implemented as a two-tier two application on Amazon EC2 instances, with a web layer and a separate database tier. As traffic rises, the organization detects severe delays in delivering timely marketing and purchase confirmation emails to consumers due to the design. The organization wishes to decrease the amount of time spent addressing difficult email delivery problems and to cut operating costs.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Correct Answer: B 

Topic 1

A business's application makes use of AWS Lambda functions. A code examination reveals that database credentials are stored in the source code of a Lambda function, violating the company's security policy. To comply with security policy requirements, credentials must be safely maintained and automatically cycled on a regular basis.

What should a solutions architect propose as the MOST SECURE method of meeting these requirements?

- A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can use the key ID to retrieve the password from CloudHSM. Use CloudHSM to automatically rotate the password.
- B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can use the secret ID to retrieve the password from Secrets Manager. Use Secrets Manager to automatically rotate the password.
- C. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can use the key ID to retrieve the password from AWS KMS. Use AWS KMS to automatically rotate the uploaded password.
- D. Move the database password to an environment variable that is associated with the Lambda function. Retrieve the password from the environment variable by invoking the function. Create a deployment script to automatically rotate the password.

Correct Answer: B 

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

Question #99

Topic 1

For each of its developer accounts, a corporation has configured AWS CloudTrail logs to transport log files to an Amazon S3 bucket. The organization has established a centralized AWS account for the purpose of facilitating administration and auditing. Internal auditors need access to CloudTrail logs, however access to all developer account users must be limited. The solution should be both secure and efficient.

How should a solutions architect address these considerations?

- A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.
- C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read-only permissions to the bucket.
- D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

Correct Answer: C 

Question #100

Topic 1

A solutions architect is improving a website in preparation for a forthcoming musical performance. Real-time streaming of the performances will be accessible, as well as on-demand viewing. The event is anticipated to draw a large internet audience from across the world.

Which service will optimize both real-time and on-demand steaming performance?

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

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

Question #101

Topic 1

A database is hosted on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that is subjected to high-volume reads. When evaluating read performance from a secondary AWS Region, application developers detect a considerable lag. The developers need a solution that has a read replication latency of less than one second.

What recommendations should the solutions architect make?

- A. Install MySQL on Amazon EC2 in the secondary Region.
- B. Migrate the database to Amazon Aurora with cross-Region replicas.
- C. Create another RDS for MySQL read replica in the secondary Region.
- D. Implement Amazon ElastiCache to improve database query performance.

Correct Answer: B 

Reference:

<https://aws.amazon.com/rds/aurora/global-database/>

Question #102

Topic 1

Currently, a business runs a web application that is backed up by an Amazon RDS MySQL database. It features daily automatic backups that are not encrypted. A security audit entails the encryption of future backups and the destruction of unencrypted backups. Before deleting the previous backups, the firm will create at least one encrypted backup.

What should be done to allow encrypted backups in the future?

- A. Enable default encryption for the Amazon S3 bucket where backups are stored.
- B. Modify the backup section of the database configuration to toggle the Enable encryption check box.
- C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.
- D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

Correct Answer: C 

However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

DB instances that are encrypted can't be modified to disable encryption.

You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.

Encrypted read replicas must be encrypted with the same key as the source DB instance when both are in the same AWS Region.

You can't restore an unencrypted backup or snapshot to an encrypted DB instance.

To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key identifier of the destination AWS Region. This is because KMS encryption keys are specific to the AWS Region that they are created in.

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Question #103

Topic 1

On AWS, a business is developing a document storage solution. The application is deployed across different Amazon EC2 Availability Zones. The firm demands a highly accessible document storage. When requested, documentation must be returned quickly. The lead engineer has setup the application to store documents in Amazon Elastic Block Store (Amazon EBS), but is open to examine additional solutions to fulfill the availability requirement.

What recommendations should a solutions architect make?

- A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.
- B. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.
- C. Use Amazon Elastic Block Store (Amazon EBS) for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.
- D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

Correct Answer: B 

Question #104

Topic 1

A solutions architect desires that all new users meet particular difficulty standards and are required to rotate their IAM user passwords on a regular basis.

What is the solution architect's role in achieving this?

- A. Set an overall password policy for the entire AWS account
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Correct Answer: A 

Question #105

Topic 1

A business uses AWS to host its website. The organization has utilized Amazon EC2 Auto Scaling to accommodate the extremely fluctuating demand. Management is worried that the firm is overprovisioning its infrastructure, particularly at the three-tier application's front end. A solutions architect's primary responsibility is to guarantee that costs are minimized without sacrificing performance.

What is the solution architect's role in achieving this?

- A. Use Auto Scaling with Reserved Instances.
- B. Use Auto Scaling with a scheduled scaling policy.
- C. Use Auto Scaling with the suspend-resume feature.
- D. Use Auto Scaling with a target tracking scaling policy.

Correct Answer: C 

Question #106

Topic 1

Each entry to a company's facility is equipped with badge readers. When badges are scanned, the readers transmit an HTTPS message indicating who tried to enter that specific entry.

A solutions architect must develop a system that will handle these sensor signals. The solution must be highly accessible, with the findings made available for analysis by the company's security staff.

Which system design should be recommended by the solutions architect?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Correct Answer: B 

Question #107

Topic 1

A business is in the process of transferring its apps to AWS. At the moment, on-premises apps create hundreds of terabytes of data, which is kept on a shared file system. The organization is using a cloud-based analytics solution to derive insights from this data on an hourly basis.

The business requires a solution to manage continuous data transfer between its on-premises shared file system and Amazon S3. Additionally, the solution must be capable of coping with brief gaps in internet access.

Which data transmission options should the business utilize to achieve these requirements?

- A. AWS DataSync
- B. AWS Migration Hub
- C. AWS Snowball Edge Storage Optimized
- D. AWS Transfer for SFTP

Correct Answer: A 

Reference:

<https://aws.amazon.com/cloud-data-migration/>

Question #108

Topic 1

On Amazon EC2 instances, a business runs an application. The application is deployed on private subnets inside the us-east-1 Region's three Availability Zones. The instances must have internet access in order to download files. The organization is looking for a design that is readily accessible across the Region.

Which solution should be done to guarantee that internet access is not disrupted?

- A. Deploy a NAT instance in a private subnet of each Availability Zone.
- B. Deploy a NAT gateway in a public subnet of each Availability Zone.
- C. Deploy a transit gateway in a private subnet of each Availability Zone.
- D. Deploy an internet gateway in a public subnet of each Availability Zone.

Correct Answer: B 

Question #109

Topic 1

An application is deployed across various Availability Zones using Amazon EC2 instances. The instances are deployed behind an Application Load Balancer in an Amazon EC2 Auto Scaling group. The program operates optimally when the CPU usage of the Amazon EC2 instances is close to or equal to 40%.

What should a solutions architect do to ensure that the required performance is maintained throughout all group instances?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B 

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 AutoScaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to: Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your AutoScaling group.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Question #110

Topic 1

The web application of a business is hosted on Amazon EC2 instances and is protected by an Application Load Balancer. The corporation recently altered its policy, requiring that the application be accessible exclusively from a single nation.

Which setup will satisfy this criterion?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Correct Answer: C 

Reference:

<https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/>

Question #111

Topic 1

AWS Lambda functions are being developed and deployed by an engineering team. The team must build roles and administer policies in AWS IAM in order to set the Lambda functions' rights.

How should the team's permissions be adjusted to correspond to the principle of least privilege?

- A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.
- B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group.
- C. Create an execution role for the Lambda functions. Attach a managed policy that has permission boundaries specific to these Lambda functions.
- D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions. Allow the engineering team to assume this role.

Correct Answer: A 

Question #112

Topic 1

A business is migrating from on-premises Oracle to Amazon Aurora PostgreSQL. Numerous apps write to the same tables in the database. The apps must be transferred sequentially, with a month between migrations. Management has raised worry about the database's heavy read and write activity. Throughout the entire migration process, the data must be maintained in sync across both databases.

What recommendations should a solutions architect make?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all cables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: B 

Question #113

Topic 1

AWS is used by an ecommerce firm to operate a multi-tier application. Amazon EC2 hosts both the front-end and back-end layers, while Amazon RDS for MySQL hosts the database. The backend tier is responsible for communication with the RDS instance. There are many requests to the database to get identical datasets, which results in performance slowdowns.

Which actions should be performed to optimize the backend's performance?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B 

Question #114

Topic 1

A solutions architect is migrating static content from an Amazon EC2 instance-hosted public website to an Amazon S3 bucket. The static assets will be distributed using an Amazon CloudFront distribution. The EC2 instances' security group limits access to a subset of IP ranges. Access to static material should be regulated in a similar manner.

Which combination of actions will satisfy these criteria? (Select two.)

- A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.
- B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.
- C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.
- D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.
- E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

Correct Answer: AB 

Question #115

Topic 1

A user owns a MySQL database, which is used by a variety of customers that anticipate a maximum delay of 100 milliseconds on queries. Once an entry is recorded in the database, it is almost never modified. Clients get access to a maximum of one record at a time.

Due to rising customer demand, database access has expanded tremendously. As a consequence, the resulting load will quickly surpass the capability of even the most costly hardware available. The user want to move to AWS and is open to experimenting with new database systems.

Which solution would resolve the database load problem and provide nearly limitless future scalability?

- A. Amazon RDS
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. AWS Data Pipeline

Correct Answer: B 

Reference:

<https://aws.amazon.com/blogs/big-data/near-zero-downtime-migration-from-mysql-to-dynamodb/>

Question #116

Topic 1

Amazon DynamoDB is being used by an entertainment firm to store media metadata. The application requires extensive reading and often encounters delays. The organization lacks the people necessary to manage extra operational expenses and requires an increase in DynamoDB's performance efficiency without changing the application.

What solution architecture approach should be recommended to satisfy this requirement?

- A. Use Amazon ElastiCache for Redis.
- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: D 

Question #117

Topic 1

In a branch office, a firm runs an application in a tiny data closet with no virtualized computing resources. The application's data is saved on a network file system (NFS) volume. Daily offsite backups of the NFS volume are required by compliance requirements.

Which solution satisfies these criteria?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Correct Answer: B 

AWS Storage Gateway Hardware Appliance

Hardware Appliance -

Storage Gateway is available as a hardware appliance, adding to the existing support for VMware ESXi, Microsoft Hyper-V, and Amazon EC2. This means that you can now make use of Storage Gateway in situations where you do not have a virtualized environment, server-class hardware or IT staff with the specialized skills that are needed to manage them. You can order appliances from Amazon.com for delivery to branch offices, warehouses, and ~~outpost~~ offices that lack dedicated IT resources. Setup (as you will see in a minute) is quick and easy, and gives you access to three storage solutions:

File Gateway – A file interface to Amazon S3, accessible via NFS or SMB. The files are stored as S3 objects, allowing you to make use of specialized S3 features such as lifecycle management and cross-region replication. You can trigger AWS Lambda functions, run Amazon Athena queries, and use Amazon Macie to discover and classify sensitive data.

Reference:

<https://aws.amazon.com/blogs/aws/new-aws-storage-gateway-hardware-appliance/> <https://aws.amazon.com/storagegateway/file/>

Question #118

Topic 1

A business is using AWS to host an election reporting website for consumers worldwide. The website makes use of Amazon EC2 instances in an Auto Scaling group with Application Load Balancers for the web and application layers. The database layer is powered by Amazon RDS for MySQL. The website is updated once an hour with election results and has previously seen hundreds of individuals check the data. The firm anticipates a big boost in demand in the coming months as a result of impending elections in many nations. A solutions architect's objective is to increase the website's capacity to manage increased demand while limiting the requirement for more EC2 instances.

Which solution will satisfy these criteria?

- A. Launch an Amazon ElastiCache cluster to cache common database queries.
- B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.
- C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.
- D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

Correct Answer: B 

Question #119

Topic 1

Amazon S3 is used by a corporation to store historical weather recordings. The records are accessed through a URL that refers to a domain name on the company's website. Subscriptions enable users from all around the globe to access this material. The organization's core domain name is hosted by a third-party supplier, although the company recently transferred some of its services to Amazon Route 53. The corporation want to consolidate contracts, minimize user latency, and lower the cost of offering the application to subscribers.

Which solution satisfies these criteria?

- A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.
- C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.
- D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

Correct Answer: B 

Question #120

Topic 1

A business is developing a web application that will be accessible over the internet. The application is hosted on Amazon EC2 for Linux instances that leverage Amazon RDS MySQL Multi-AZ DB instances to store sensitive user data. Public subnets are used for EC2 instances, whereas private subnets are used for RDS DB instances. The security team has required that web-based attacks on database instances be prevented.

What recommendations should a solutions architect make?

- A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.
- C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.
- D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

Correct Answer: C 

Question #121

Topic 1

A solutions architect is responsible for designing a solution for migrating a persistent database from on-premises to AWS. According to the database administrator, the database needs 64,000 IOPS. If feasible, the database administrator wishes to host the database instance on a single Amazon Elastic Block Store (Amazon EBS) volume.

Which option satisfies the database administrator's requirements the most effectively?

- A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.
- B. Create a Nitro-based Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.
- C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.
- D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

Correct Answer: B 

Question #122

Topic 1

A solutions architect is tasked with the responsibility of creating the architecture for a new application that will be deployed to the AWS Cloud. Amazon EC2 On-Demand Instances will be used to execute the application, which will automatically scale across different Availability Zones. Throughout the day, the EC2 instances will scale up and down periodically. The load distribution will be handled by an Application Load Balancer (ALB). The architecture must be capable of managing dispersed session data. The firm is ready to make necessary adjustments to the code.

What is the solution architect's responsibility in ensuring that the design enables distributed session data management?

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

Correct Answer: A 

Question #123

Topic 1

Multiple Amazon EC2 Linux instances are used by a business in a VPC to execute applications that need a hierarchical directory structure. The apps must be able to access and write to shared storage fast and simultaneously.

How is this accomplished?

- A. Create an Amazon Elastic File System (Amazon EFS) file system and mount it from each EC2 instance.
- B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.
- C. Create a file system on an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes attached to each EC2 instance. Synchronize the Amazon Elastic Block Store (Amazon EBS) volumes across the different EC2 instances.

Correct Answer: A 

Question #124

Topic 1

A business maintains monthly phone records. Statistically, recorded data may be referred to randomly within a year but is seldom retrieved beyond that time period.

Files less than a year old must be queried and retrieved immediately. It is okay for there to be a delay in obtaining older files. A solutions architect must ensure that the captured data is stored at the lowest possible cost.

Which option is the MOST CHEAPEST?

- A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier Query S3 Glacier tags and retrieve the files from S3 Glacier.
- B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.
- C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

Correct Answer: B 

Question #125

Topic 1

A business wants to move a workload to AWS. The chief information security officer demands that any data stored in the cloud be encrypted at rest. The organization desires total control over the encryption key lifecycle management process.

Independent of AWS CloudTrail, the organization must be able to promptly delete key material and audit key use. The selected services should interface with other AWS storage services.

Which services adhere to these security standards?

- A. AWS CloudHSM with the CloudHSM client
- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

Correct Answer: A 

Question #126

Topic 1

A business hosts an application on Amazon Web Services (AWS) and utilizes Amazon DynamoDB as the database. To handle data from the database, the organization adds Amazon EC2 instances to a private network. The organization connects to DynamoDB using two NAT instances. The corporation want to decommission its NAT instances. A solutions architect must develop a solution that connects to DynamoDB and is self-managing.

Which approach is the MOST cost-effective in terms of meeting these requirements?

- A. Create a gateway VPC endpoint to provide connectivity to DynamoDB.
- B. Configure a managed NAT gateway to provide connectivity to DynamoDB.
- C. Establish an AWS Direct Connect connection between the private network and DynamoDB.
- D. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB.

Correct Answer: B 

Question #127

Topic 1

A business administers its own Amazon EC2 instances, which are configured to operate MySQL databases. The firm manages replication and scaling manually as demand grows or falls. The organization need a new solution that makes it easier to add or remove computing resources from its database layer as required. Additionally, the solution must increase speed, scalability, and durability with little work on the part of operations.

Which solution satisfies these criteria?

- A. Migrate the databases to Amazon Aurora Serverless for Aurora MySQL.
- B. Migrate the databases to Amazon Aurora Serverless for Aurora PostgreSQL.
- C. Combine the databases into one larger MySQL database. Run the larger database on larger EC2 instances.
- D. Create an EC2 Auto Scaling group for the database tier. Migrate the existing databases to the new environment.

Correct Answer: D 

Reference:

[\(p.6\)](https://aws-quickstart.s3.amazonaws.com/quickstart-drupal/doc/drupal-on-the-aws-cloud.pdf)

Question #128

Topic 1

A business want to transfer two apps to AWS. Both apps handle a huge number of files concurrently by accessing the same files. Both programs must read files with a minimum of delay.

Which architecture would a solutions architect suggest in this case?

- A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.
- B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.
- C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.
- D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

Correct Answer: D 

Question #129

Topic 1

A corporation operates a containerized application in an on-premises data center using a Kubernetes cluster. The organization stores data in a MongoDB database.

The organization want to transition some of these environments to AWS, but no modifications to the code or deployment methods are currently feasible. The business need a solution that lowers operating costs.

Which solution satisfies these criteria?

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage.
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Correct Answer: C 

Question #130

Topic 1

A business has a mobile chat application that utilizes an Amazon DynamoDB data storage. Users want as low delay as possible while reading fresh messages. A solutions architect's objective is to provide the optimum solution with the fewest possible application modifications.

Which technique should be chosen by the solutions architect?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Correct Answer: A 

Reference:

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-accelerator-dax-in-memory-caching-for-read-intensive-workloads/>

Question #131

Topic 1

A solutions architect must offer a fully managed alternative to an on-premises system that enables file interchange between workers and partners. Workers connecting from on-premises systems, remote employees, and external partners must have easy access to the solution.

Which solution satisfies these criteria?

- A. Use AWS Transfer for SFTP to transfer files into and out of Amazon S3.
- B. Use AWS Snowball Edge for local storage and large-scale data transfers.
- C. Use Amazon FSx to store and transfer files to make them available remotely.
- D. Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.

Correct Answer: A 

Reference:

<https://aws.amazon.com/aws-transfer-family/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Question #132

Topic 1

A business is operating an application on Amazon EC2 instances on a private subnet. The program must be capable of storing and retrieving data from Amazon S3. To save expenses, the corporation wishes to optimize the configuration of its AWS resources.

How should the business go about doing this?

- A. Deploy a NAT gateway to access the S3 buckets.
- B. Deploy AWS Storage Gateway to access the S3 buckets.
- C. Deploy an S3 gateway endpoint to access the S3 buckets.
- D. Deploy an S3 interface endpoint to access the S3 buckets.

Correct Answer: B 

Question #133

Topic 1

AWS is used by a business to store user data. The data is continually accessed, with peak consumption occurring during work hours. Access patterns vary, with some data going months without being accessed. A solutions architect must pick a solution that is both cost efficient and durable, while also maintaining a high degree of availability.

Which storage option satisfies these criteria?

- A. Amazon S3 Standard
- B. Amazon S3 Intelligent-Tiering
- C. Amazon S3 Glacier Deep Archive
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B 

Question #134

Topic 1

A solutions architect must create a managed storage system that supports high-performance machine learning for a company's application. This application runs on AWS Fargate, and the storage attached to it must support concurrent file access and provide good speed.

Which storage choice should the architect of solutions recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon Elastic File System (Amazon EFS).
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon Elastic Block Store (Amazon EBS).

Correct Answer: B 

Question #135

Topic 1

A business is considering migrating a classic application to AWS. Currently, the application communicates with an on-premises storage system through NFS. The program cannot be changed to perform this function using any other communication protocol than NFS.

Which storage solution, if any, should a solutions architect propose for post-migration use?

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

Correct Answer: C 

Question #136

Topic 1

A business wishes to run its mission-critical apps in containers in order to fulfill scalability and availability requirements. The corporation would rather concentrate on key application maintenance. The firm does not want to be responsible for provisioning and maintaining the containerized workload's underlying infrastructure.

What actions should a solutions architect take to ensure that these criteria are met?

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

Correct Answer: C 

Reference:

<https://aws.amazon.com/fargate/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc&fargate-blogs.sort-by=item.additionalFields.createdDate&fargate-blogs.sort-order=desc>

Question #137

Topic 1

On an Amazon RDS MySQL DB instance, a company's production application processes online transaction processing (OLTP) transactions. The firm is also offering a new reporting tool with the same data access. The reporting tool must be highly accessible and have no adverse effect on the production application's performance.

How is this accomplished?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Correct Answer: B 

Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/#:~>

Question #138

Topic 1

A business operates a service that generates event data. The firm wishes to use AWS for the purpose of processing event data as it is received. The data is structured in a certain sequence that must be preserved during processing. The firm wishes to deploy a solution with the lowest possible operating costs.

How is this to be accomplished by a solution architect?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A 

Question #139

Topic 1

A business is installing an application that handles near-real-time streaming data. The workload will be run on Amazon EC2 instances. The network architecture must be configured in such a way that the latency between nodes is as minimal as feasible.

Which network solution combination will suit these requirements? (Select two.)

- A. Enable and configure enhanced networking on each EC2 instance.
- B. Group the EC2 instances in separate accounts.
- C. Run the EC2 instances in a cluster placement group.
- D. Attach multiple elastic network interfaces to each EC2 instance.
- E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

Correct Answer: CD 

Question #140

Topic 1

A business maintains on-premises servers that operate a relational database. The existing database handles a large volume of read requests from users in various places. The organization want to transition to AWS with little effort. The database solution should enable catastrophe recovery while minimizing disruption to the business's present traffic flow.

Which solution satisfies these criteria?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
- B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Correct Answer: A 

Reference:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

Question #141

Topic 1

On Amazon EC2, a business hosts an ecommerce application. The application is composed of a stateless web layer that needs a minimum of ten instances and a maximum of 250 instances to run. 80% of the time, the program needs 50 instances.

Which solution should be adopted in order to keep expenses down?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Correct Answer: D 

Reserved Instances -

Having 50 EC2 RIs provide a discounted hourly rate and an optional capacity reservation for EC2 instances. AWS Billing automatically applies your RI's discounted rate when attributes of EC2 instance usage match attributes of an active RI.

If an Availability Zone is specified, EC2 reserves capacity matching the attributes of the RI. The capacity reservation of an RI is automatically utilized by running instances matching these attributes.

You can also choose to forego the capacity reservation and purchase an RI that is scoped to a region. RIs that are scoped to a region automatically apply the RI's discount to instance usage across AZs and instance sizes in a region, making it easier for you to take advantage of the RI's discounted rate.

On-Demand Instance -

On-Demand instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

The pricing below includes the cost to run private and public AMIs on the specified operating system (Windows Usage prices apply to Windows Server 2003 R2,

2008, 2008 R2, 2012, 2012 R2, 2016, and 2019). Amazon also provides you with additional instances for Amazon EC2 running Microsoft Windows with SQL

Server, Amazon EC2 running SUSE Linux Enterprise Server, Amazon EC2 running Red Hat Enterprise Linux and Amazon EC2 running IBM that are priced differently.

Spot Instances -

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your

Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

Reference:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

<https://aws.amazon.com/ec2/pricing/on-demand/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

Question #142

Topic 1

A business uses two Amazon EC2 instances to run a dynamic web application. The organization has its own SSL certificate, which is used to complete SSL termination on each instance.

Recently, there has been an increase in traffic, and the operations team concluded that SSL encryption and decryption is causing the web servers' compute capacity to surpass its limit.

What should a solutions architect do to optimize the performance of an application?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
- B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
- C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
- D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Correct Answer: D 

Question #143

Topic 1

A corporation is doing an evaluation of an existing workload placed on AWS using the AWS Well-Architected Framework. The evaluation discovered a public-facing website operating on the same Amazon EC2 instance as a freshly installed Microsoft Active Directory domain controller to support other AWS services. A solutions architect must offer a new design that increases the architecture's security and reduces the administrative burden on IT workers.

What recommendations should the solutions architect make?

- A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.
- B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.
- C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
- D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.

Correct Answer: A 

AWS Managed Microsoft AD -

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2012 R2. When you select and launch this directory type, it is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC). The domain controllers run in different Availability Zones in a region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you.

Reference:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

Question #144

Topic 1

The database of a business is hosted in the us-east-1 Region on an Amazon Aurora MySQL DB cluster. The database is around 4 terabytes in size. The company's disaster recovery plan should be expanded to include the us-west-2 region. The firm must be able to fail over to us-west-2 within a 15-minute recovery time goal (RTO).

What recommendations should a solutions architect make to satisfy these requirements?

- A. Create a Multi-Region Aurora MySQL DB cluster in us-east-1 and use-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.
- B. Take a snapshot of the DB cluster in us-east-1. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to copy the snapshot to us-west-2 and restore the snapshot in us-west-2 when failure is detected.
- C. Create an AWS CloudFormation script to create another Aurora MySQL DB cluster in us-west-2 in case of failure. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to deploy the AWS CloudFormation stack in us-west-2 when failure is detected.
- D. Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Configure an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function upon receipt of resource events. Configure the Lambda function to promote the DB cluster in us-west-2 when failure is detected.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/aws-backup/latest/devguide/eventbridge.html>

Question #145

Topic 1

Amazon Aurora was recently selected as the data repository for a company's worldwide ecommerce platform. When developers run extensive reports, they discover that the ecommerce application is performing badly. When monthly reports are performed, a solutions architect notices that the ReadIOPS and CPUUtilization metrics spike.

Which approach is the MOST cost-effective?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.
- D. Increase the Provisioned IOPS on the Aurora instance.

Correct Answer: D 

Question #146

Topic 1

A business's backup data totals 700 terabytes (TB) and is kept in network attached storage (NAS) at its data center. This backup data must be available in the event of occasional regulatory inquiries and preserved for a period of seven years. The organization has chosen to relocate its backup data from its on-premises data center to Amazon Web Services (AWS). Within one month, the migration must be completed. The company's public internet connection provides 500 Mbps of dedicated capacity for data transport.

What should a solutions architect do to ensure that data is migrated and stored at the LOWEST possible cost?

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

Correct Answer: A 

Question #147

Topic 1

A business outsources its marketplace analytics management to a third-party partner. The vendor requires restricted programmatic access to the company's account's resources. All necessary policies have been established to ensure acceptable access.

Which new component provides the vendor the MOST SECURE access to the account?

- A. Create an IAM user.
- B. Implement a service control policy (SCP)
- C. Use a cross-account role with an external ID.
- D. Configure a single sign-on (SSO) identity provider.

Correct Answer: B 

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html#data-from-iam

Question #148

Topic 1

The main and secondary data centers of a business are located 500 miles (804.7 kilometers) apart and are linked through high-speed fiber-optic cable. For a mission-critical workload, the organization requires a highly available and secure network link between its data centers and an AWS VPC. A solutions architect must choose a connectivity solution that is as resilient as possible.

Which solution satisfies these criteria?

- A. Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
- B. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
- C. Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
- D. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Correct Answer: D 

Question #149

Topic 1

The dynamic website of a business is hosted on-premises in the United States. The firm is expanding throughout Europe and want to reduce site loading speeds for new European visitors. The backbone of the website must stay in the United States. A few days from now, the product will be introduced, and an instant answer is required.

What recommendations should the solutions architect make?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

Correct Answer: C 

Question #150

Topic 1

A corporation used an AWS Direct Connect connection to copy 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region. The business now wishes to replicate the data in another S3 bucket located in the us-west-2 Region. AWS Snowball is not permitted at the colocation facility.

What should a solutions architect suggest as a means of achieving this?

- A. Order a Snowball Edge device to copy the data from one Region to another Region.
- B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.
- C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.
- D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

Correct Answer: D 

Question #151

Topic 1

A solutions architect must verify that API requests to Amazon DynamoDB are not routed across the internet from Amazon EC2 instances inside a VPC.

What is the solution architect's role in achieving this? (Select two.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create a new DynamoDB table that uses the endpoint.
- D. Create an ENI for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the default security group to provide access.

Correct Answer: AB 

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Gateway endpoints -

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3 -

DynamoDB -

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Question #152

Topic 1

A business wishes to migrate live datasets online from an on-premises NFS server to an Amazon S3 bucket called DOC-EXAMPLE-BUCKET.

Verification of data integrity is essential both during and after the transmission. Additionally, the data must be encrypted.

A solutions architect is migrating the data using an AWS solution.

Which solution satisfies these criteria?

- A. AWS Storage Gateway file gateway
- B. S3 Transfer Acceleration
- C. AWS DataSync
- D. AWS Snowball Edge Storage Optimized

Correct Answer: C 

Reference:

<https://aws.amazon.com/blogs/storage/transferring-data-between-aws-accounts-using-aws-datasync/>

Question #153

Topic 1

A business wishes to migrate its on-premises network-attached storage (NAS) to Amazon Web Services (AWS). The corporation wishes to make the data accessible to any Linux instance inside its VPC and to guarantee that changes to the data store are immediately synced across all instances that use it. The bulk of data is viewed infrequently, whereas certain files are read concurrently by numerous people.

Which option satisfies these criteria and is the MOST cost-effective?

- A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.
- B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after the appropriate number of days.
- C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.
- D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

Correct Answer: D 

Question #154

Topic 1

Each month, a business must create sales reports. On the first day of each month, the reporting procedure starts 20 Amazon EC2 instances. The procedure lasts seven days and cannot be paused. The corporation wishes to keep expenses low.

Which pricing strategy should the business pursue?

- A. Reserved Instances
- B. Spot Block Instances
- C. On-Demand Instances
- D. Scheduled Reserved Instances

Correct Answer: D 

Explanation -

Scheduled Reserved Instances -

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled

Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

If you require a capacity reservation on a continuous basis, Reserved Instances might meet your needs and decrease costs.

How Scheduled Instances Work -

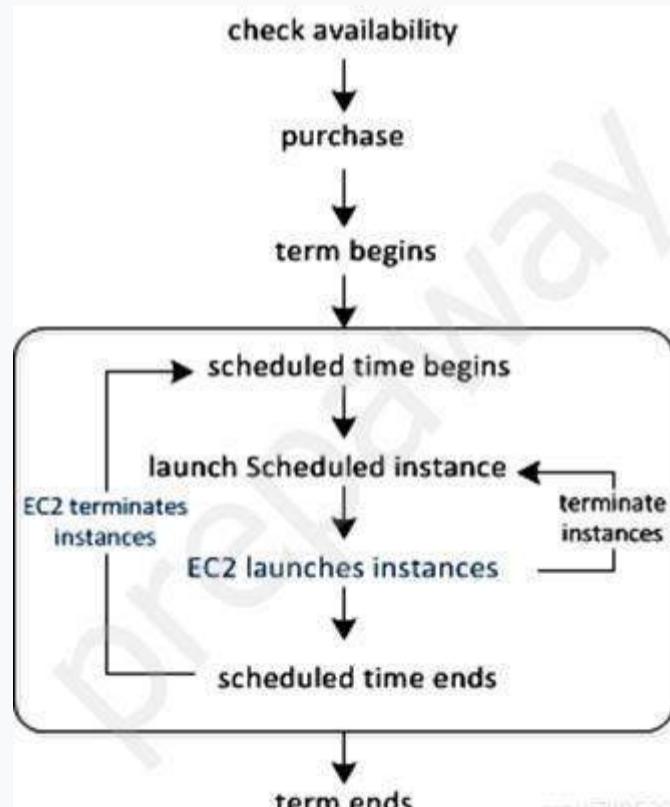
Amazon EC2 sets aside pools of EC2 instances in each Availability Zone for use as Scheduled Instances. Each pool supports a specific combination of instance type, operating system, and network.

To get started, you must search for an available schedule. You can search across multiple pools or a single pool. After you locate a suitable schedule, purchase it.

You must launch your Scheduled Instances during their scheduled time periods, using a launch configuration that matches the following attributes of the schedule that you purchased: instance type, Availability Zone, network, and platform. When you do so, Amazon EC2 launches EC2 instances on your behalf, based on the specified launch specification. Amazon EC2 must ensure that the EC2 instances have terminated by the end of the current scheduled time period so that the capacity is available for any other Scheduled Instances it is reserved for. Therefore, Amazon EC2 terminates the EC2 instances three minutes before the end of the current scheduled time period.

You can't stop or reboot Scheduled Instances, but you can terminate them manually as needed. If you terminate a Scheduled Instance before its current scheduled time period ends, you can launch it again after a few minutes. Otherwise, you must wait until the next scheduled time period.

The following diagram illustrates the lifecycle of a Scheduled Instance.



Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Question #155**Topic 1**

A business offers an online service for uploading and transcoding video material for usage on any mobile device. The application design makes use of Amazon Elastic File System (Amazon EFS) Standard to gather and store the films so that they may be processed by numerous Amazon EC2 Linux instances. As the service's popularity has increased, the storage charges have become prohibitively costly.

Which storage option is the MOST CHEAPEST?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon Elastic File System (Amazon EFS) for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

Correct Answer: A **Question #156****Topic 1**

Each day, a corporation gets ten terabytes of instrumentation data from many machines situated in a single plant. The data is saved in JSON files on a storage area network (SAN) inside the factory's on-premises data center. The organization want to upload this data to Amazon S3 so that it may be accessible by a number of other systems that do crucial near-real-time analytics. Because the data is deemed sensitive, a secure transmission is critical.

Which option provides the MOST SECURE method of data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: D **Question #157****Topic 1**

A data science team needs storage to analyze logs on a nightly basis. The amount and quantity of logs are unclear, however they will be retained for 24 hours.

Which approach is the MOST cost-effective?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B 

Reference:

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

Question #158

Topic 1

A development team is releasing a new product on AWS, and as part of the rollout, they are using AWS Lambda. For one of the Lambda functions, the team allocates 512 MB of RAM. The function is finished in two minutes with this memory allocation. Monthly, the function is executed millions of times, and the development team is worried about the cost. The team does experiments to determine the effect of various Lambda memory allocations on the function's cost.

Which measures will result in a decrease in the product's Lambda costs? (Select two.)

- A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.
- B. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 90 seconds.
- C. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 4 minutes.
- D. Increase the memory allocation for this Lambda function to 2,048 MB if this change causes the execution time of each function to be less than 1 minute.
- E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

Correct Answer: AE 

Question #159

Topic 1

A business is using a centralized Amazon Web Services account to store log data in many Amazon S3 buckets. Prior to uploading data to S3 buckets, a solutions architect must guarantee that the data is encrypted at rest. Additionally, data must be encrypted during transit.

Which solution satisfies these criteria?

- A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
- D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>

Question #160

Topic 1

A business requires the migration of a Microsoft Windows-based application to AWS. This program utilizes a shared Windows file system that is tied to numerous Amazon EC2 Windows machines.

What actions should a solutions architect take to achieve this?

- A. Configure a volume using Amazon Elastic File System (Amazon EFS). Mount the EFS volume to each Windows instance.
- B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.
- C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: C 

Question #161

Topic 1

An IAM group is associated with the following IAM policy. This is the group's sole policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "1",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        }  
    ]  
}
```

praw709528

What are the policy's effective IAM permissions for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Correct Answer: D 

Question #162

Topic 1

A business is searching for a solution that would enable them to store video archives created from archived news footage on AWS. The business must keep expenses down and will seldom need to recover these data. When files are required, they must be provided within a five-minute window.

Which approach is the MOST cost-effective?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A 

Question #163

Topic 1

A business utilizes Application Load Balancers (ALBs) across many AWS Regions. The ALBs experience fluctuating traffic throughout the year. The company's networking personnel must enable connection by allowing the ALBs' IP addresses over the on-premises firewall.

Which solution is the MOST scalable and requires the least amount of setup changes?

- A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
- B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
- C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
- D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall's rule to allow the Elastic IP address attached to the NLB.

Correct Answer: C 

Question #164

Topic 1

Multiple Linux Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes are used by a company's web application. The organization is searching for a solution that will boost the application's resilience in the event of a failure and will offer storage that adheres to the atomicity, consistency, isolation, and durability requirements (ACID).

What actions should a solutions architect take to ensure that these criteria are met?

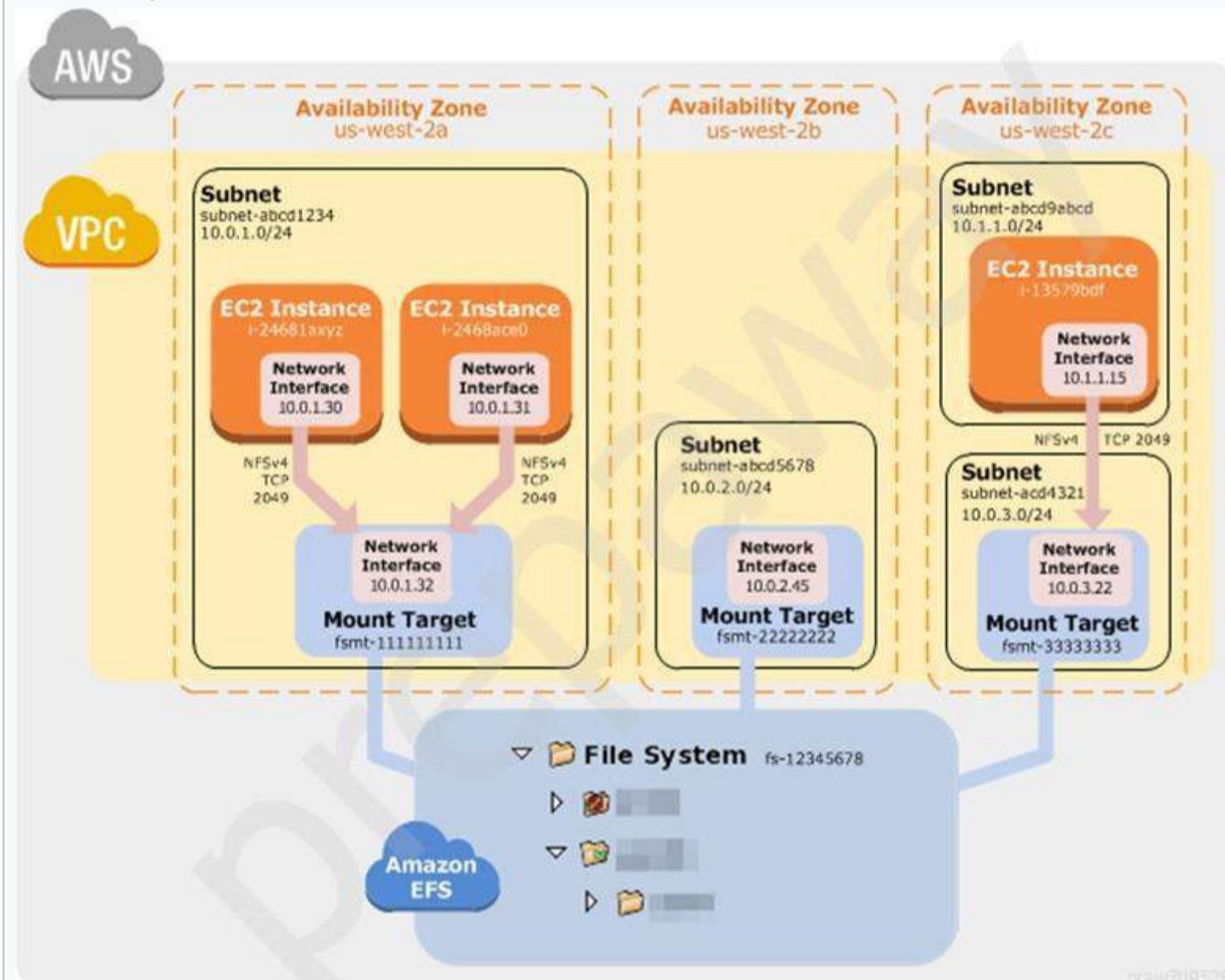
- Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
- Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
- Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon Elastic File System (Amazon EFS) and mount a target on each instance.
- Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: C 

How Amazon EFS Works with Amazon EC2

The following illustration shows an example VPC accessing an Amazon EFS file system. Here, EC2 instances in the VPC have file systems mounted.

In this illustration, the VPC has three Availability Zones, and each has one mount target created in it. We recommend that you access the file system from a mount target within the same Availability Zone. One of the Availability Zones has two subnets. However, a mount target is created in only one of the subnets.



Benefits of Auto Scaling -

Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it.

You can also configure Amazon EC2 Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Amazon EC2 Auto Scaling can launch instances in another one to compensate.

Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of capacity to handle the current traffic demand.

Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you save money by launching instances when they are needed and terminating them when they aren't.

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2>
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

Question #165**Topic 1**

Under its registered parent domain, a firm hosts many websites for various lines of business. According to the subdomain, anyone visiting these websites will be directed to the proper backend Amazon EC2 instance. Static webpages, pictures, and server-side programming such as PHP and JavaScript are all hosted on the websites.

Certain websites see a spike in traffic during the first two hours of business, followed by consistent use throughout the remainder of the day. A solutions architect must build a system that adapts capacity automatically to certain traffic patterns while being cost effective.

Which AWS service or feature combination will suit these requirements? (Select two.)

- A. AWS Batch
- B. Network Load Balancer
- C. Application Load Balancer
- D. Amazon EC2 Auto Scaling
- E. Amazon S3 website hosting

Correct Answer: DE **Question #166****Topic 1**

As a web application, a corporation has built a new video game. The application is deployed in a three-tier design using Amazon RDS for MySQL in a VPC. Multiple players will compete simultaneously online through the database layer. The makers of the game want to show a top-10 scoreboard in near-real time and to enable players to pause and resume the game while retaining their existing scores.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Correct Answer: D 

Question #167

Topic 1

For many years, a business has stored analytics data on an Amazon RDS instance. The firm hired a solutions architect to develop an API that would enable consumers to access this data. The program is expected to have periods of idleness but may get surges of traffic within seconds.

Which option should the architect recommend?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions.
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Correct Answer: C 

AWS Lambda -

With Lambda, you can run code for virtually any type of application or backend service – all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

How it works -



Amazon API Gateway -

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and

WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

Reference:

<https://aws.amazon.com/lambda/>

<https://aws.amazon.com/api-gateway/>

Question #168

Topic 1

A mobile gaming startup uses Amazon EC2 instances to host application servers. Every 15 minutes, the servers get updates from players. The mobile game generates a JSON object containing the game's progress since the last update and delivers it to an Application Load Balancer. As the mobile game is played, it loses game updates. The business intends to develop a long-lasting method for older devices to get updates.

What should a solution architect propose for system decoupling?

- A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.
- B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.
- D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

Correct Answer: C 

Question #169

Topic 1

The application of a business is hosted on Amazon EC2 instances that are part of an Auto Scaling group behind an Elastic Load Balancer. Each year, the firm predicts a rise in traffic over a holiday, based on the application's history. A solutions architect must develop a plan to guarantee that the Auto Scaling group raises capacity proactively in order to minimize any effect on application users' performance.

Which solution will satisfy these criteria?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2_INSTANCE_LAUNCH events.

Correct Answer: B 

Question #170

Topic 1

A firm that now hosts a web application on-premises is ready to migrate to AWS and launch a newer version of the program. The organization must route requests depending on the URL query string to either the AWS- or on-premises-hosted application. The on-premises application is inaccessible over the internet, and a VPN connection between Amazon VPC and the company's data center is formed. The firm intends to deploy this application using an Application Load Balancer (ALB).

Which solution satisfies these criteria?

- A. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to each target group of each ALB. Route with Amazon Route 53 based on the URL query string.
- B. Use two ALBs: one for on-premises and one for the AWS resource. Add hosts to the target group of each ALB. Create a software router on an EC2 instance based on the URL query string.
- C. Use one ALB with two target groups: one for the AWS resource and one for on premises. Add hosts to each target group of the ALB. Configure listener rules based on the URL query string.
- D. Use one ALB with two AWS Auto Scaling groups: one for the AWS resource and one for on premises. Add hosts to each Auto Scaling group. Route with Amazon Route 53 based on the URL query string.

Correct Answer: A 

Question #171

Topic 1

A recent review of a company's IT spending demonstrates the critical necessity of lowering backup costs. The chief information officer of the organization want to simplify the on-premises backup architecture and cut expenses by phasing out physical backup tapes. The company's current investment in on-premises backup systems and procedures must be protected.

What recommendations should a solutions architect make?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon Elastic File System (Amazon EFS) file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon Elastic File System (Amazon EFS) file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Correct Answer: D 

Question #172

Topic 1

A business maintains an internal web-based application. The application is deployed on Amazon EC2 instances that are routed via an Application Load Balancer. The instances are distributed across several Availability Zones through an Amazon EC2 Auto Scaling group. During business hours, the Auto Scaling group grows up to 20 instances, then scales down to two instances overnight. Staff are saying that the program is very sluggish to start the day, but performs fine by mid-morning.

How might the scale be altered to accommodate employee concerns while keeping expenses low?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

Question #173

Topic 1

A business must adhere to a regulatory obligation that all emails be saved and preserved outside for a period of seven years. An administrator has prepared compressed email files on-premises and wishes to have the data transferred to AWS storage through a managed service.

Which managed service should be recommended by a solutions architect?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon S3 Glacier
- C. AWS Backup
- D. AWS Storage Gateway

Correct Answer: D 

Reference:

<https://aws.amazon.com/storagegateway/faqs/>

Question #174

Topic 1

A business hosts its website on Amazon EC2 instances that are distributed across several Availability Zones through an Elastic Load Balancer. The instances are managed as part of an EC2 Auto Scaling group. The website stores product manuals for download through Amazon Elastic Block Store (Amazon EBS) volumes. The organization often changes the product information, which means that new instances created by the Auto Scaling group frequently have out-of-date data. It may take up to 30 minutes for all changes to be received by fresh instances. Additionally, the changes involve resizing the EBS volumes during business hours.

The corporation want to guarantee that product manuals are constantly current and that the architecture adapts fast to rising customer demand. A solutions architect must satisfy these objectives without requiring the business to upgrade its application code or website.

What actions should the solutions architect take to achieve this objective?

- A. Store the product manuals in an EBS volume. Mount that volume to the EC2 instances.
- B. Store the product manuals in an Amazon S3 bucket. Redirect the downloads to this bucket.
- C. Store the product manuals in an Amazon Elastic File System (Amazon EFS) volume. Mount that volume to the EC2 instances.
- D. Store the product manuals in an Amazon S3 Standard-Infrequent Access (S3 Standard-IA) bucket. Redirect the downloads to this bucket.

Correct Answer: B 

Question #175

Topic 1

A business intends to install an Amazon RDS database instance powered by Amazon Aurora. The organization has a 90-day backup retention policy.

Which solution, if any, should a solutions architect suggest?

- A. Set the backup retention period to 90 days when creating the RDS DB instance.
- B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.
- C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days. Create an AWS Backup job to schedule the execution of the backup plan daily.
- D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot. Purge snapshots older than 90 days.

Correct Answer: B 

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html

Question #176

Topic 1

A solutions architect is configuring a virtual private cloud (VPC) with public and private subnets. The VPC and subnets are configured using IPv4 CIDR blocks. Each of the three Availability Zones (AZs) has one public and one private subnet. An internet gateway is used to connect public subnets to the internet. Private subnets must have internet connectivity in order for Amazon EC2 instances to obtain software upgrades.

What should the solutions architect do to allow private subnets to connect to the internet?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress- only internet gateway.

Correct Answer: A 

Question #177

Topic 1

Currently, a corporation has 250 TB of backup data saved in Amazon S3 using a vendor-specific format. The firm wishes to extract files from Amazon S3, convert them to an industry-standard format, and then re-upload them to Amazon S3. The firm want to reduce the costs connected with data transmission for this session.

What actions should a solutions architect take to achieve this?

- A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.
- B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and re-upload the files to Amazon S3 from the virtual machine.
- C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.
- D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re- upload the files to Amazon S3 from the EC2 instance.

Correct Answer: D 

Question #178

Topic 1

A business's applications are hosted on on-premises servers. The corporation is rapidly depleting its storage capacity. The programs make use of both block and network file storage. The business need a high-performance solution that enables local caching without requiring it to re-architect its current applications.

Which steps should a solutions architect perform in combination to satisfy these requirements? (Select two.)

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Correct Answer: DE 

Question #179

Topic 1

A business hosts a web service on Amazon EC2 instances that are routed via an Application Load Balancer. The instances are distributed across two Availability Zones through an Amazon EC2 Auto Scaling group. At all times, the corporation requires a minimum of four instances to achieve the needed service level agreement (SLA) requirements while keeping expenses low.

How can the organization maintain compliance with the SLA if an Availability Zone fails?

- A. Add a target tracking scaling policy with a short cooldown period.
- B. Change the Auto Scaling group launch configuration to use a larger instance type.
- C. Change the Auto Scaling group to use six servers across three Availability Zones.
- D. Change the Auto Scaling group to use eight servers across two Availability Zones.

Correct Answer: A 

Question #180

Topic 1

A firm is using the AWS Cloud to run a three-tier ecommerce application. The firm hosts the website on Amazon S3 and combines it with a sales API. The API is hosted by the firm on three Amazon EC2 instances that are connected through an Application Load Balancer (ALB). The API is composed of static and dynamic front-end content, as well as back-end workers that asynchronously execute sales requests. The corporation anticipates a big and abrupt surge in sales requests during events celebrating the introduction of new items.

What should a solutions architect prescribe to assure the effective processing of all requests?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

Correct Answer: D 

Reference:

<https://aws.amazon.com/sqs/>

Question #181

Topic 1

Amazon EC2 instances are used to execute an application. The application's sensitive data is housed in an Amazon S3 bucket. The bucket must be shielded from internet access while yet allowing access to it for services inside the VPC.

Which activities should solutions architected take in order to do this? (Select two.)

- A. Create a VPC endpoint for Amazon S3.
- B. Enable server access logging on the bucket.
- C. Apply a bucket policy to restrict access to the S3 endpoint.
- D. Add an S3 ACL to the bucket that has sensitive information.
- E. Restrict users using the IAM policy to use the specific bucket.

Correct Answer: AC 

Question #182

Topic 1

A business's program creates a vast number of files, each around 5 MB in size. Amazon S3 is used to store the files. According to company policy, files must be retained for a period of four years before they may be erased. Immediate access is always essential due to the fact that the files contain vital business data that is difficult to replicate. The files are commonly viewed within the first 30 days after the establishment of the item, but are seldom accessed beyond that time period.

Which storage option is the MOST CHEAPEST?

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

Correct Answer: C 

Question #183

Topic 1

A business has a bucket on Amazon S3 that includes mission-critical data. The firm wishes to safeguard this data against inadvertent deletion. The data should remain available, and the user should be able to erase it on purpose.

Which actions should a solutions architect use in conjunction to achieve this? (Select two.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Correct Answer: AB 

Reference:

<https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-LNMknp7BP01IYVSlee8/Final%20practice%20exam>

Question #184

Topic 1

The HTTP application of a business is protected by a Network Load Balancer (NLB). The target group for the NLB is set to utilize an Amazon EC2 Auto Scaling group that has numerous EC2 instances that operate the web service. The firm sees that the application's HTTP faults are not being detected by the NLB. These problems need a manual restart of the web service's EC2 instances. The organization wants to increase the availability of the program without having to write bespoke scripts or code.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
- B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
- C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
- D. Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Correct Answer: C 

Question #185

Topic 1

A business maintains an application that processes incoming communications. These messages are then digested in a matter of seconds by dozens of other apps and microservices.

The quantity of communications fluctuates significantly and sometimes peaks above 100,000 per second. The firm wishes to divorce the solution from its underlying infrastructure and thereby boost its scalability.

Which solution satisfies these criteria?

- A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.
- B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

Correct Answer: A 

Reference:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

Question #186

Topic 1

On AWS, a business operates a high-performance computing (HPC) workload. The demand necessitated low network latency and high network throughput through closely linked node-to-node communication. Amazon EC2 instances are started with default configurations and are appropriately scaled for computation and storage capabilities.

What should a solutions architect advise to optimize the workload's performance?

- A. Choose a cluster placement group while launching Amazon EC2 instances.
- B. Choose dedicated instance tenancy while launching Amazon EC2 instances.
- C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.
- D. Choose the required capacity reservation while launching Amazon EC2 instances.

Correct Answer: A 

Question #187

Topic 1

A business has two applications: one that sends messages with payloads to be processed and another that receives messages with payloads. The organization wishes to create an Amazon Web Services (AWS) solution to manage communications between the two apps. The sender program is capable of sending around 1,000 messages every hour. Processing of communications may take up to two days. If the messages do not process, they must be kept to avoid interfering with the processing of subsequent messages.

Which solution satisfies these parameters and is the MOST OPTIMAL in terms of operational efficiency?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Correct Answer: C 

Question #188

Topic 1

A business uses a VPC that is provisioned with a CIDR block of 10.10.1.0/24. Due to continuing expansion, this block's IP address space may soon be consumed. A solutions architect must expand the VPC's IP address capacity.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Create a new VPC. Associate a larger CIDR block.
- B. Add a secondary CIDR block of 10.10.2.0/24 to the VPC.
- C. Resize the existing VPC CIDR block from 10.10.1.0/24 to 10.10.1.0/16.
- D. Establish VPC peering with a new VPC that has a CIDR block of 10.10.1.0/16.

Correct Answer: A 

Question #189

Topic 1

A business hosts its website on Amazon EC2 instances that are routed via an ELB Application Load Balancer. The DNS is handled via Amazon Route 53. The firm want to establish a backup website with a message, phone number, and email address for users to contact in the event that the original website becomes unavailable.

How should this solution be implemented?

- A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.
- B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.
- C. Deploy the application in another AWS Region and use ELB health checks for failover routing.
- D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

Correct Answer: A 

Question #190

Topic 1

A firm's on-premises business program creates hundreds of files daily. These files are kept on an SMB file share and need a connection to the application servers with a low latency. A new business policy requires that all files created by applications be moved to AWS. A VPN connection to AWS is already established.

The application development team lacks the time required to modify the application's code in order to migrate it to AWS.

Which service should a solutions architect propose to enable an application to transfer files to Amazon Web Services (AWS)?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Windows File Server
- C. AWS Snowball
- D. AWS Storage Gateway

Correct Answer: B 

Reference:

<https://aws.amazon.com/blogs/storage/accessing-smb-file-shares-remotely-with-amazon-fsx-for-windows-file-server/>

Question #191

Topic 1

A business uses WebSockets to host a live chat application on its on-premises servers. The firm want to transfer the application to Amazon Web Services (AWS).

Traffic to the application is uneven, and the firm anticipates more traffic with sudden spikes in the future.

The business need a highly scalable solution that requires minimal server maintenance or sophisticated capacity planning.

Which solution satisfies these criteria?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
- B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

Correct Answer: B 

Question #192

Topic 1

A business intends to migrate many gigabytes of data to AWS. Offline data is obtained from ships. Before transmitting the data, the organization want to do complicated transformations.

Which Amazon Web Services (AWS) service should a solutions architect suggest for this migration?

- A. AWS Snowball
- B. AWS Snowmobile
- C. AWS Snowball Edge Storage Optimize
- D. AWS Snowball Edge Compute Optimize

Correct Answer: D 

Question #193

Topic 1

A business is transferring its infrastructure from on-premises to the AWS Cloud. One of the company's apps stores data on a Windows file server farm that utilizes Distributed File System Replication (DFSR) to maintain data consistency. The file server farm must be replaced by a solutions architect.

Which solution architect service should be used?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Correct Answer: B 

Migrating Existing Files to Amazon FSx for Windows File Server Using AWS DataSync

We recommend using AWS DataSync to transfer data between Amazon FSx for Windows File Server file systems. DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and other AWS storage services over the internet or

AWS Direct Connect. DataSync can transfer your file system data and metadata, such as ownership, time stamps, and access permissions.

Reference:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

Question #194

Topic 1

Two video conversion programs are being used by a media organization on Amazon EC2 instances. One utility is Windows-based, while the other is Linux-based. Each video file is rather huge and both programs must process it.

The organization requires a storage solution that enables the creation of a centralized file system that can be mounted on all of the EC2 instances utilized in this operation.

Which solution satisfies these criteria?

- A. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.
- B. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.
- C. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances
- D. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.

Correct Answer: C 

Question #195

Topic 1

A business uses Amazon RDS to power a web application. A fresh database administrator mistakenly deleted data from a database table. To aid in recovery from such an occurrence, the organization desires the capacity to restore the database to the condition it was in five minutes prior to any alteration during the past 30 days.

Which capability should the solutions architect include into the design to satisfy this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

Correct Answer: C 

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html

Question #196

Topic 1

A business is building a video converter application that will be hosted on AWS. The program will be offered in two flavors: a free version and a premium version. People on the premium tier will get their videos converted first, followed by users on the tree tier.

Which option satisfies these criteria and is the MOST cost-effective?

- A. One FIFO queue for the paid tier and one standard queue for the free tier.
- B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.
- D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

Correct Answer: D 

Question #197

Topic 1

A business has an application that sends messages to Amazon Simple Queue Service. Another program polls the queue and performs I/O-intensive operations on the messages. The organization has a service level agreement (SLA) that stipulates the maximum time allowed between message receipt and response to users. Due to the rise in message volume, the organization is having trouble fulfilling its SLA on a constant basis.

What should a solutions architect do to assist in increasing the application's processing speed and ensuring that it can manage any level of load?

- A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.
- B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance.
- C. Create an Amazon Machine image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy to keep its aggregate CPU utilization below 70%.
- D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

Correct Answer: D 

Question #198

Topic 1

In the AWS Cloud, a business is operating a multi-tier ecommerce web application. The application is hosted on Amazon EC2 instances that are connected to an Amazon RDS MySQL Multi-AZ database. Amazon RDS is setup with the latest generation instance and 2,000 GB of storage in a General Purpose SSD (gp2) volume from Amazon Elastic Block Store (Amazon EBS). During moments of heavy demand, the database performance has an effect on the application.

After studying the logs in Amazon CloudWatch Logs, a database administrator discovers that when the number of read and write IOPS exceeds 6,000, the application's performance constantly drops.

What should a solutions architect do to optimize the performance of an application?

- A. Replace the volume with a Magnetic volume.
- B. Increase the number of IOPS on the gp2 volume.
- C. Replace the volume with a Provisioned IOPS (PIOPS) volume.
- D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

Correct Answer: C 

Question #199

Topic 1

Recently, a business introduced a new form of internet-connected sensor. The business anticipates selling thousands of sensors that are intended to feed large amounts of data to a central location every second. A solutions architect must develop a system that ingests and stores data in near-real time with millisecond responsiveness for engineering teams to examine.

Which solution should the architect of solutions recommend?

- A. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- B. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.
- C. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.
- D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

Correct Answer: D 

Question #200

Topic 1

A business must share an Amazon S3 bucket with a third-party provider. All items must be accessible to the bucket owner.

Which procedure should be followed in order to share the S3 bucket?

- A. Update the bucket to be a Requester Pays bucket.
- B. Update the bucket to enable cross-origin resource sharing (CORS).
- C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.
- D. Create an IAM policy to require users to grant bucket-owner-full-control when uploading objects.

Correct Answer: C 

By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. To get access to the object, the object owner must explicitly grant you (the bucket owner) access. The object owner can grant the bucket owner full control of the object by updating the access control list (ACL) of the object. The object owner can update the ACL either during a put or copy operation, or after the object is added to the bucket.

Similar:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-require-object-ownership/>

Resolution Add a bucket policy that grants users access to put objects in your bucket only when they grant you (the bucket owner) full control of the object.

Reference:

<https://aws.amazon.com/it/premiumsupport/knowledge-center/s3-bucket-owner-access/>

Question #201

Topic 1

A business developed a meal ordering application that collects and maintains user data for future research. The static front end of the application is hosted on an Amazon EC2 instance. The front-end application communicates with the back-end application, which is hosted on a different EC2 instance. The data is subsequently stored in Amazon RDS by the backend application.

What should a solutions architect do to decouple and scalability the architecture?

- A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.
- B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.
- C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.
- D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

Correct Answer: D 

Question #202

Topic 1

A business stores static photos for its website in an Amazon S3 bucket. Permissions were specified to restrict access to Amazon S3 items to privileged users only.

What steps should a solutions architect take to prevent data loss? (Select two.)

- A. Enable versioning on the S3 bucket.
- B. Enable access logging on the S3 bucket.
- C. Enable server-side encryption on the S3 bucket.
- D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.
- E. Use MFA Delete to require multi-factor authentication to delete an object.

Correct Answer: AE 

Question #203

Topic 1

A solutions architect is developing a document review application that will be stored in an Amazon S3 bucket. The solution must prevent unintentional document deletion and guarantee that all document versions are accessible. The ability for users to download, change, and upload documents is required.

Which measures should be conducted in combination to achieve these requirements? (Select two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD 

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

To customize your data retention approach and control storage costs, use object versioning with Object lifecycle management. For information about creating S3

Lifecycle policies using the AWS Management Console, see How Do I Create a Lifecycle Policy for an S3 Bucket? in the Amazon Simple Storage Service Console

User Guide.

If you have an object expiration lifecycle policy in your non-versioned bucket and you want to maintain the same permanent delete behavior when you enable versioning, you must add a noncurrent expiration policy. The noncurrent expiration lifecycle policy will manage the deletes of the noncurrent object versions in the version-enabled bucket. (A version-enabled bucket maintains one current and zero or more noncurrent object versions.)

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key. Enabling and suspending versioning is done at the bucket level. When you enable versioning on an existing bucket, objects that are already stored in the bucket are unchanged. The version IDs (null), contents, and permissions remain the same. After you enable S3 Versioning for a bucket, each object that is added to the bucket gets a version ID, which distinguishes it from other versions of the same key.

Only Amazon S3 generates version IDs, and they can't be edited. Version IDs are Unicode, UTF-8 encoded, URL-ready, opaque strings that are no more than

1,024 bytes long. The following is an example: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dlbrHY+MTRCx3vjVBH40Nr8X8gdRQBpUMLUo.

Using MFA delete -

If a bucket's versioning configuration is MFA Delete-enabled, the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket. Requests that include x-amz-mfa must use HTTPS. The header's value is the concatenation of your authentication device's serial number, a space, and the authentication code displayed on it. If you do not include this request header, the request fails.

Reference:

<https://aws.amazon.com/s3/features/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Question #204

Topic 1

A corporation hosts more than 300 websites and apps on a worldwide scale. Each day, the organization wants a platform capable of analyzing more than 30 TB of clickstream data.

What should a solutions architect do with the clickstream data during transmission and processing?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Correct Answer: C 

Question #205

Topic 1

A business is developing a three-tier online application that will include a web server, an application server, and a database server. While packages are being delivered, the program will monitor their GPS locations. The database will be updated every 0-5 seconds by the program.

Tracking information must be read as quickly as possible to allow users to verify the status of their deliveries. On certain days, just a few parcels may be monitored, while on others, millions of packages may be tracked. The tracking system must be searchable using the tracking ID, the customer ID, and the order ID. Orders placed after one month will no longer be monitored.

What should a solution architect propose in order to do this with the lowest possible total cost of ownership?

- A. Use Amazon DynamoDB Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.
- B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.
- C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.
- D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

Correct Answer: B 

Question #206

Topic 1

A news organization with correspondents located around the globe uses AWS to host its broadcast system. The reporters provide the broadcast system with live feeds. The reporters transmit live broadcasts through the Real Time Messaging Protocol using software installed on their phones (RTMP).

A solutions architect must provide a system that enables reporters to deliver the highest-quality streams possible. The solution must ensure that TCP connections to the broadcast system are expedited.

What approach should the solutions architect use in order to satisfy these requirements?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. AWS Client VPN
- D. Amazon EC2 instances and AWS Elastic IP addresses

Correct Answer: A 

Reference:

<https://aws.amazon.com/solutions/implementations/live-streaming-on-aws/>

Question #207

Topic 1

A business is transferring a set of Linux-based web servers to AWS. For certain content, the web servers must access files stored in a shared file storage. To fulfill the migration deadline, only minor adjustments are necessary.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Create an Amazon S3 Standard bucket with access to the web server.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) volume and mount it on all web servers.
- D. Configure Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1) volumes and mount them on all web servers.

Correct Answer: C 

Question #208

Topic 1

Every day, a business gets structured and semi-structured data from a variety of sources. A solutions architect must create a solution that makes use of frameworks for big data processing. SQL queries and business intelligence tools should be able to access the data.

What should the solutions architect advocate in order to provide the MOST performant solution possible?

- A. Use AWS Glue to process data and Amazon S3 to store data.
- B. Use Amazon EMR to process data and Amazon Redshift to store data.
- C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.
- D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

Correct Answer: B 

Reference:

<https://aws.amazon.com/redshift/features/>

Question #209

Topic 1

A MySQL database instance on Amazon RDS is used by an application. The RDS database is rapidly depleting its storage capacity. A solutions architect wants to expand disk capacity without causing downtime.

Which method satisfies these criteria with the MINIMUM amount of effort?

- A. Enable storage auto scaling in RDS.
- B. Increase the RDS database instance size.
- C. Change the RDS database instance storage type to Provisioned IOPS.
- D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

Correct Answer: C 

Question #210

Topic 1

A corporation want to move a 143 TB MySQL database to AWS. The objective is to continue using Amazon Aurora MySQL as the platform. The organization connects to Amazon VPC using a 100 Mbps AWS Direct Connect connection.

Which option best satisfies the requirements of the business and requires the LEAST amount of time?

- A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.
- B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.
- C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.
- D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

Correct Answer: D 

Question #211

Topic 1

A business runs an ecommerce application in a single VPC. A single web server and an Amazon RDS Multi-AZ database instance comprise the application stack.

Twice a month, the firm introduces new items. This results in a 400% increase in website traffic for a minimum of 72 hours. Users' browsers encounter poor response times and numerous timeout issues during product launches.

What should a solutions architect do to minimize response times and timeout failures while maintaining a minimal operational overhead?

- A. Increase the instance size of the web server.
- B. Add an Application Load Balancer and an additional web server.
- C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.
- D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

Correct Answer: A 

Question #212

Topic 1

A solutions architect is developing a two-step order process application. The first step is synchronous and must return with minimal delay to the user. Because the second stage is more time consuming, it will be done as a distinct component. Orders must be processed precisely once and in their original sequence of receipt.

How are these components to be integrated by the solutions architect?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

Question #213

Topic 1

A business is using AWS to operate an application that processes weather sensor data stored in an Amazon S3 bucket. Three batch tasks are scheduled to run hourly to process data in the S3 bucket for various reasons. The organization wishes to minimize total processing time by employing an event-based strategy to run the three programs in parallel.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Subscribe all applications to the queue for processing.
- B. Enable S3 Event Notifications for new objects to an Amazon Simple Queue Service (Amazon SQS) standard queue. Create an additional SQS queue for all applications, and subscribe all applications to the initial queue for processing.
- C. Enable S3 Event Notifications for new objects to separate Amazon Simple Queue Service (Amazon SQS) FIFO queues. Create an additional SQS queue for each application, and subscribe each queue to the initial topic for processing.
- D. Enable S3 Event Notifications for new objects to an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon Simple Queue Service (Amazon SQS) queue for each application, and subscribe each queue to the topic for processing.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ways-to-add-notification-config-to-bucket.html>

Question #214

Topic 1

Multiple Amazon EC2 instances in a single Availability Zone are used by a gaming firm to host a multiplayer game that connects with players using Layer 4 communication. The chief technology officer (CTO) desires a highly accessible and cost-effective architecture.

What actions should a solutions architect take to ensure that these criteria are met? (Select two.)?

- A. Increase the number of EC2 instances.
- B. Decrease the number of EC2 instances.
- C. Configure a Network Load Balancer in front of the EC2 instances.
- D. Configure an Application Load Balancer in front of the EC2 instances.
- E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

Correct Answer: CE 

Network Load Balancer overview -

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.

When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. For more information, see Availability Zones.

If you enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone, this increases the fault tolerance of your applications. For example, if one or more target groups does not have a healthy target in an Availability Zone, we remove the

IP address for the corresponding subnet from DNS, but the load balancer nodes in the other Availability Zones are still available to route traffic.

If a client doesn't honor the time-to-live (TTL) and sends requests to the IP address after it is removed from DNS, the requests fail.

For TCP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, destination port, and TCP sequence number. The TCP connections from a client have different source ports and sequence numbers, and can be routed to different targets. Each individual TCP connection is routed to a single target for the life of the connection.

For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

Question #215

Topic 1

A business runs a static website on Amazon S3. A solutions architect must guarantee that data is recoverable in the event of an accidentally deleted file.

Which action is necessary to achieve this?

- A. Enable Amazon S3 versioning.
- B. Enable Amazon S3 Intelligent-Tiering.
- C. Enable an Amazon S3 lifecycle policy.
- D. Enable Amazon S3 cross-Region replication.

Correct Answer: A 

Data can be recovered if versioning is enabled, as it provides extra protection like file delete, MFA delete. MFA Delete only works for CLI or API interaction, not in the

AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Object Versioning -

[1]

(version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Reference:

<https://books.google.com.sg/books?id=wv45DQAAQBAJ&pg=PA39&lpg=PA39&dq=hosts+a+static+website+within+an+Amazon+S3+bucket.+A+solutions+architect+needs+to+ensure+that+data+can+be+recovered+in+case+of+accidental+deletion&source=bl&ots=0NolP5igY5&sig=ACfU3U3opL9Jha6jM2EI8x7EcjK4rigQHQ&hl=en&sa=X&ved=2ahUKEwiS9e3yy7vpAhVx73MBHZNoDnQQ6AEwAH>

[oECBQQAQ#v=onepage&q=hosts%20a%20static%20website%20within%20an%20Amazon%20S3%20bucket.%20A%20solutions%20architect%20needs%20to](https://books.google.com.sg/books?id=wv45DQAAQBAJ&pg=PA39&lpg=PA39&dq=hosts+a+static+website+within+an+Amazon+S3+bucket.%20A%20solutions%20architect%20needs%20to)

[%20ensure%20that%20data%20can%20be%20recovered%20in%20case%20of%20accidental%20deletion&f=false](https://books.google.com.sg/books?id=wv45DQAAQBAJ&pg=PA39&lpg=PA39&dq=hosts+a+static+website+within+an+Amazon+S3+bucket.%20A%20solutions%20architect%20needs%20to+ensure%20that%20data%20can%20be%20recovered%20in%20case%20of%20accidental%20deletion&f=false)

<https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html>

Question #216

Topic 1

A firm gathers data on temperature, humidity, and air pressure in cities across the world. Each day, an average of 500 GB of data is gathered each station. Each location is equipped with a high-speed internet connection. The company's weather forecasting tools are regionally focused and do daily data analysis.

What is the SPEEDIEST method for collecting data from all of these worldwide sites?

- A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.
- B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.
- D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

Correct Answer: A 

Step-1: To transfer to S3 from global sites: Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront's™ globally distributed AWS Edge Locations. Used to accelerate object uploads to S3 over long distances (latency). Transfer acceleration is as secure as a direct upload to S3.

Step-2: When the application analyze/aggregate the data from S3 and then again upload the results - Multipart upload

Reference:

<http://lavnish.blogspot.com/2017/06/aws-s3-cross-region-replication.html> <https://aws.amazon.com/s3/transfer-acceleration/>

Question #217

Topic 1

A business uses an Amazon EC2 instance to host a web server on a public subnet with an Elastic IP address. The EC2 instance is assigned to the default security group. The default network access control list (ACL) has been updated to deny all traffic. A solutions architect must ensure that the web server is accessible from any location through port 443.

Which sequence of procedures will achieve this objective? (Select two.)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

Correct Answer: AE 

Question #218

Topic 1

A business has developed a three-tiered picture sharing platform. It runs the front-end layer on one Amazon EC2 instance, the backend layer on another, and the MySQL database on a third. A solutions architect has been entrusted with the responsibility of developing a solution that is highly available and needs the fewest modifications to the application as possible.

Which solution satisfies these criteria?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Correct Answer: D 

Question #219

Topic 1

A business has developed a virtual private cloud (VPC) with various private subnets distributed across different Availability Zones (AZs) and one public subnet located in one of the AZs. A NAT gateway is launched on the public subnet. Within private subnets, there are circumstances when a NAT gateway is used to connect to the internet. In the event of an AZ failure, the organization wants to verify that not all instances have internet connection difficulties and that a backup plan is prepared.

Which solution, according to a solutions architect, is the MOST highly available?

- A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.
- B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.
- C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.
- D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

Correct Answer: C 

Question #220

Topic 1

A business maintains numerous AWS accounts and deploys apps in the us-west-2 Region. Each account's application logs are kept in Amazon S3 buckets. The organization wishes to create a centralized log analysis system based on a single Amazon S3 bucket. Logs cannot depart us-west-2, and the corporation want to incur the fewest possible operating costs.

Which option satisfies these criteria and is the MOST cost-effective?

- A. Create an S3 Lifecycle policy that copies the objects from one of the application S3 buckets to the centralized S3 bucket.
- B. Use S3 Same-Region Replication to replicate logs from the S3 buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
- C. Write a script that uses the PutObject API operation every day to copy the entire contents of the buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
- D. Write AWS Lambda functions in these accounts that are triggered every time logs are delivered to the S3 buckets (s3:ObjectCreated:* event). Copy the logs to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

Correct Answer: A 

Reference:

<https://www.varonis.com/blog/how-to-use-aws-s3/>

Question #221

Topic 1

A business is migrating its on-premises apps to Amazon Elastic Compute Cloud instances. However, due to variable compute needs, EC2 instances must always be available for usage between the hours of 8 a.m. and 5 p.m. in designated Availability Zones.

Which Amazon Elastic Compute Cloud instances should the business use to execute the applications?

- A. Scheduled Reserved Instances
- B. On-Demand Instances
- C. Spot Instances as part of a Spot Fleet
- D. EC2 instances in an Auto Scaling group

Correct Answer: A 

Question #222

Topic 1

A solutions architect is developing a solution that entails coordinating a number of Amazon Elastic Container Service (Amazon ECS) task types that are operating on Amazon EC2 instances that are members of an ECS cluster. All tasks' output and status data must be saved. Each job outputs around 10 MB of data, and hundreds of tasks may be operating concurrently. The system should be tuned for reading and writing at a fast rate of speed. As ancient

Because outputs are preserved and removed, the total storage space should not exceed 1 TB.

Which storage option should be recommended by the solutions architect?

- A. An Amazon DynamoDB table accessible by all ECS cluster instances.
- B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.
- C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.
- D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

Correct Answer: C 

Question #223

Topic 1

A business uses AWS Organizations in conjunction with two AWS accounts: Logistics and Sales. The Logistics account is responsible for the operation of an Amazon Redshift cluster. Amazon EC2 instances are included in the Sales account. The Sales account requires access to the Amazon Redshift cluster maintained by the Logistics account.

What should a solutions architect propose as the MOST cost-effective way to accomplish this requirement?

- A. Set up VPC sharing with the Logistics account as the owner and the Sales account as the participant to transfer the data.
- B. Create an AWS Lambda function in the Logistics account to transfer data to the Amazon EC2 instances in the Sales account.
- C. Create a snapshot of the Amazon Redshift cluster, and share the snapshot with the Sales account. In the Sales account, restore the cluster by using the snapshot ID that is shared by the Logistics account.
- D. Run COPY commands to load data from Amazon Redshift into Amazon S3 buckets in the Logistics account. Grant permissions to the Sales account to access the S3 buckets of the Logistics account.

Correct Answer: C 

Reference:

<https://www.sqlshack.com/share-aws-redshift-data-across-accounts/>

Question #224

Topic 1

A solutions architect must design a bastion host architecture that is highly available. The solution must be robust inside a single AWS Region and need little maintenance effort.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.
- B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.
- C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.
- D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

Correct Answer: D 

Question #225

Topic 1

A business is developing a massively multiplayer online game. The game communicates through UDP, thus it is critical that the client and backend have a low latency. The backend is hosted on Amazon EC2 instances that may be scaled across various AWS Regions. The firm requires a high level of availability for the game in order for consumers worldwide to have access to it at all times.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Deploy Amazon CloudFront to support the global traffic. Configure CloudFront with an origin group to allow access to EC2 instances in multiple Regions.
- B. Deploy an Application Load Balancer in one Region to distribute traffic to EC2 instances in each Region that hosts the game's backend instances.
- C. Deploy Amazon CloudFront to support an origin access identity (OAI). Associate the OAI with EC2 instances in each Region to support global traffic.
- D. Deploy a Network Load Balancer in each Region to distribute the traffic. Use AWS Global Accelerator to route traffic to the correct Regional endpoint.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

Question #226

Topic 1

A business wishes to relocate its accounting system from an on-premises data center to an AWS Region. Priority one should be given to data security and an unalterable audit log. The organization must conduct compliance audits on all AWS operations. Although the organization has activated AWS CloudTrail, it wants to ensure that it complies with these criteria.

Which safeguards and security measures should a solutions architect use to safeguard and secure CloudTrail? (Select two.)

- A. Enable CloudTrail log file validation.
- B. Install the CloudTrail Processing Library.
- C. Enable logging of Insights events in CloudTrail.
- D. Enable custom logging from the on-premises resources.
- E. Create an AWS Config rule to monitor whether CloudTrail is configured to use server-side encryption with AWS KMS managed encryption keys (SSE-KMS).

Correct Answer: AC 

Question #227

Topic 1

A solutions architect is developing a new service to be used in conjunction with Amazon API Gateway. The service's request patterns will be erratic, ranging from zero to over 500 per second. The entire quantity of data that must be persisted in a backend database is now less than 1 GB, with unpredictability about future expansion. Simple key-value queries may be used to query data.

Which AWS service combination would best suit these requirements? (Select two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Correct Answer: BC 

Reference:

<https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-api-gateway-supports-endpoint-integrations-with-private-vpcs>

Question #228

Topic 1

Management has chosen to allow IPv6 on all AWS VPCs. After a period of time, a solutions architect attempts to create a new instance and gets an error indicating that the subnet does not have enough accessible IP address space.

What is the solution architect's role in resolving this?

- A. Check to make sure that only IPv6 was used during the VPC creation.
- B. Create a new IPv4 subnet with a larger range, and then launch the instance.
- C. Create a new IPv6-only subnet with a large range, and then launch the instance.
- D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

Correct Answer: C 

Question #229

Topic 1

For the last 15 years, a corporation has been operating a web application using an Oracle relational database in an on-premises data center. The company's database must be migrated to AWS. The organization need a way to cut operating costs without modifying the application's code.

Which solution satisfies these criteria?

- A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.
- B. Use Amazon EC2 instances to migrate and operate the database servers.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.
- D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html>

Question #230**Topic 1**

A business's customer relationship management (CRM) application stores data on an Amazon RDS database instance running Microsoft SQL Server. The database is administered by the company's information technology personnel. The database includes confidential information. The organization want to guarantee that data is inaccessible to IT professionals and is only seen by authorized people.

What steps should a solutions architect take to safeguard data?

- A. Use client-side encryption with an Amazon RDS managed key.
- B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.
- C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.
- D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

Correct Answer: C **Question #231****Topic 1**

Drones are being used by a disaster response team to take photographs of recent storm damage. The reaction team's laptops lack the necessary storage and processing capacity to transmit and analyze the photographs. While the team use Amazon EC2 instances and Amazon S3 buckets for processing, network connection is inconsistent and unstable. The photos must be analysed in order to determine the extent of the damage.

What recommendations should a solutions architect make?

- A. Use AWS Snowball Edge devices to process and store the images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.
- D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

Correct Answer: A **Question #232****Topic 1**

The security team of a corporation wants that network traffic be logged in VPC Flow Logs. The logs will be viewed often for 90 days and then occasionally afterwards.

What should a solutions architect do when customizing the logs to satisfy these requirements?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Correct Answer: D 

Question #233

Topic 1

The operations team of a business already has an Amazon S3 bucket set to send notifications to an Amazon SQS queue when new items are generated in the bucket. Additionally, the development team want to get notifications when new objects are generated. The present workflow of the operations team must be maintained.

Which solution would meet these criteria?

- A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.
- B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.
- C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.
- D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

Correct Answer: D 

Question #234

Topic 1

A solutions architect is creating storage for an Amazon Linux-based high performance computing (HPC) environment. The workload saves and analyzes a huge number of engineering drawings, which necessitates the use of shared storage and high-performance computation.

Which storage choice is the best?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Lustre
- C. Amazon EC2 instance store
- D. Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io1)

Correct Answer: B 

Explanation -

Amazon FSx for Lustre -

Amazon FSx for Lustre is a new, fully managed service provided by AWS based on the Lustre file system. Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

FSx for Lustre allows customers to create a Lustre filesystem on demand and associate it to an Amazon S3 bucket. As part of the filesystem creation, Lustre reads the objects in the buckets and adds that to the file system metadata. Any Lustre client in your VPC is then able to access the data, which gets cached on the high-speed Lustre filesystem. This is ideal for HPC workloads, because you can get the speed of an optimized Lustre file system without having to manage the complexity of deploying, optimizing, and managing the Lustre cluster.

Additionally, having the filesystem work natively with Amazon S3 means you can shut down the Lustre filesystem when you don't need it but still access objects in

Amazon S3 via other AWS Services. FSx for Lustre also allows you to also write the output of your HPC job back to Amazon S3.

Reference:

https://d1.awsstatic.com/whitepapers/AWS%20Partner%20Network_HPC%20Storage%20Options_2019_FINAL.pdf

(p.8)

Question #235

Topic 1

A business is planning to build a public-facing web application on Amazon Web Services (AWS). The architecture comprises of Amazon EC2 instances contained inside a Virtual Private Cloud (VPC) and protected by an Elastic Load Balancer (ELB). The DNS is managed by a third-party provider. The solutions architect of the business must offer a solution for detecting and defending against large-scale DDoS assaults.

Which solution satisfies these criteria?

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

Correct Answer: C 

Question #236

Topic 1

A business is shifting to the Amazon Web Services (AWS) Cloud. The initial workload to move is a file server. The file share must be accessible through the Server Message Block (SMB) protocol.

Which AWS managed service satisfies these criteria?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon EC2
- C. Amazon FSx
- D. Amazon S3

Correct Answer: C 

Question #237

Topic 1

Amazon Route 53 latency-based routing is being used by a firm to route requests to their UDP-based application for customers worldwide. The program is hosted on redundant servers inside the company's own data centers in the United States, Asia, and Europe. The application must be hosted on-premises in accordance with the company's compliance standards. The organization want to enhance the application's performance and availability.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Correct Answer: C 

Question #238

Topic 1

A business is deploying a new application on an Amazon Elastic Container Service (Amazon ECS) cluster, using the Fargate ECS task launch type. The firm is monitoring CPU and memory use in anticipation of the program receiving a significant volume of traffic upon launch. However, the corporation desires cost savings as usage declines.

What recommendations should a solutions architect make?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

Correct Answer: D 

Question #239

Topic 1

A business has an AWS-hosted website. The database backend is hosted on Amazon RDS for MySQL and consists of a main instance and five read replicas to accommodate scalability requirements. To provide a consistent user experience, read replicas should be no more than one second behind the original instance.

As the website's traffic continues to grow, the copies lag farther behind at peak moments, resulting in user complaints when searches return inconsistent results. A solutions architect's goal should be to minimize replication latency with little modifications to the application's code or operational requirements.

Which solution satisfies these criteria?

- A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.
- C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.
- D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on- demand capacity scaling enabled.

Correct Answer: B 

Question #240

Topic 1

A business has users from all over the world using an application that is installed in many AWS Regions, exposing public static IP addresses. When users use the program through the internet, they encounter performance issues.

What should a solutions architect propose as a means of lowering internet latency?

- A. Set up AWS Global Accelerator and add endpoints.
- B. Set up AWS Direct Connect locations in multiple Regions.
- C. Set up an Amazon CloudFront distribution to access an application.
- D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

Correct Answer: A 

Question #241

Topic 1

A business is using an Amazon S3 bucket to store data that has been submitted by several departments from various locations. The finance manager finds that 10 TB of S3 Standard storage data has been charged each month during an AWS Well-Architected assessment. However, executing the command to select all files and folders in the AWS Management Console for Amazon S3 results in a total size of 5 TB.

What may be the potential reasons for this discrepancy? (Select two.)

- A. Some files are stored with deduplication.
- B. The S3 bucket has versioning enabled.
- C. There are incomplete S3 multipart uploads.
- D. The S3 bucket has AWS Key Management Service (AWS KMS) enabled.
- E. The S3 bucket has Intelligent-Tiering enabled.

Correct Answer: AB 

Question #242

Topic 1

On AWS, a business is creating an ecommerce website. This website is constructed on a three-tier design that contains a MySQL database in an Amazon Aurora MySQL Multi-AZ deployment. The internet application must be highly available, and will be deployed in an AWS Region with three Availability Zones initially. The program generates a statistic that indicates the amount of load it is experiencing.

Which solution satisfies these criteria?

- A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling
- B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.
- C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.
- D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

Correct Answer: B 

Question #243

Topic 1

A gaming firm uses AWS to host a browser-based application. The application's users consume a high volume of movies and photographs stored on Amazon S3. This material is consistent across all users.

The program has grown in popularity, with millions of users accessing these media files on a daily basis. The firm wants to provide files to consumers while minimizing strain on the origin.

Which option best fits these criteria in terms of cost-effectiveness?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Correct Answer: B 

Reference:

<https://aws.amazon.com/getting-started/hands-on/deliver-content-faster/>

Question #244

Topic 1

For its ecommerce website, a business developed a multi-tier application. The website makes use of a public subnet-based Application Load Balancer, a public subnet-based web tier, and a private subnet-based MySQL cluster hosted on Amazon EC2 instances. The MySQL database must obtain product catalog and price information from a third-party provider's website. A solutions architect must develop a plan that optimizes security while minimizing operating costs.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Correct Answer: C 

Question #245

Topic 1

Every day, a business processes data. The processes' output is kept in an Amazon S3 bucket, examined daily for one week, and then must remain readily available for ad hoc examination.

Which storage option is the MOST cost-effective alternative to the existing configuration?

- A. Configure a lifecycle policy to delete the objects after 30 days.
- B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.
- C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Correct Answer: D 

Question #246

Topic 1

A firm is using AWS to create a multi-instance application that needs low latency between the instances.

What recommendations should a solutions architect make?

- A. Use an Auto Scaling group with a cluster placement group.
- B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.
- C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.
- D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

Correct Answer: A 

Question #247

Topic 1

Recently, a corporation debuted a new service involving medical imaging. The firm scans the photos and transfers them to Amazon EC2 instances through an AWS Direct Connect link from its on-premises data center. Once the photos have been processed, they are placed in an Amazon S3 bucket.

According to a corporate requirement, EC2 instances cannot be accessed over the internet. The EC2 instances are contained inside a private subnet that defaults to the on-premises data center for outbound internet connectivity.

The new service is fast gaining traction. A solutions architect must offer a solution that satisfies the business's needs while also lowering Direct Connect fees.

Which approach achieves these objectives MOST EFFECTIVELY?

- A. Configure a VPC endpoint for Amazon S3. Add an entry to the private subnet's route table for the S3 endpoint.
- B. Configure a NAT gateway in a public subnet. Configure the private subnet's route table to use the NAT gateway.
- C. Configure Amazon S3 as a file system mount point on the EC2 instances. Access Amazon S3 through the mount.
- D. Move the EC2 instances into a public subnet. Configure the public subnet route table to point to an internet gateway.

Correct Answer: B 

Question #248

Topic 1

A corporation needs to create a relational database with a 1 second Recovery Point Objective (RPO) and a 1 minute Recovery Time Objective (RTO) for multi-region disaster recovery.

Which AWS solution is capable of doing this?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon RDS for MySQL with Multi-AZ enabled
- D. Amazon RDS for MySQL with a cross-Region snapshot copy

Correct Answer: A 

Question #249

Topic 1

A solutions architect is tasked with the responsibility of designing the implementation of a new static website. The solution must be cost effective and maintain a minimum of 99 percent availability.

Which solution satisfies these criteria?

- A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.
- B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.
- C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.
- D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

Correct Answer: A 

Question #250

Topic 1

A business operates a three-tier web application for the purpose of processing credit card payments. Static websites comprise the front-end user interface. The application layer may include lengthy procedures. MySQL is used in the database layer. Currently, the application is running on a single huge general-purpose Amazon EC2 machine. A solutions architect must decouple the services in order to maximize the availability of the web application.

Which of the following solutions would give the HIGHEST level of availability?

- A. Move static assets to Amazon CloudFront. Leave the application in EC2 in an Auto Scaling group. Move the database to Amazon RDS to deploy Multi-AZ.
- B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.
- C. Move static assets to Amazon S3. Move the application to AWS Lambda with the concurrency limit set. Move the database to Amazon DynamoDB with on-demand enabled.
- D. Move static assets to Amazon S3. Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled. Move the database to Amazon RDS to deploy Multi-AZ.

Correct Answer: A 

Question #251

Topic 1

A development team keeps the user name and password for its Amazon RDS MySQL DB instance in a configuration file. The configuration file is saved in plaintext on the team's Amazon EC2 instance's root device disk. When the team's application needs to connect to the database, the file is read and the credentials are loaded into the code. The team adjusted the configuration file's permissions so that only the program may access its contents. A solution architect's primary responsibility is to build a better secure system.

What actions should the solutions architect do in order to satisfy this requirement?

- A. Store the configuration file in Amazon S3. Grant the application access to read the configuration file.
- B. Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.
- C. Enable SSL connections on the database instance. Alter the database user to require SSL when logging in.
- D. Move the configuration file to an EC2 instance store, and create an Amazon Machine Image (AMI) of the instance. Launch new instances from this AMI.

Correct Answer: D 

Question #252

Topic 1

Amazon S3 is being used by a solutions architect to develop the storage architecture for a new digital media application. The media files must be robust in the event of an Availability Zone failure. Certain files are routinely visited, while others are viewed infrequently and in an unexpected fashion. The architect of the solution must keep the expenses of storing and retrieving media files to a minimum.

Which storage choice satisfies these criteria?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B 

Question #253

Topic 1

Monthly reports are stored in an Amazon S3 bucket by a company's financial application. The vice president of finance has directed that all access to these reports be documented, as well as any adjustments to the log files.

What activities can a solutions architect take to ensure compliance with these requirements?

- A. Use S3 server access logging on the bucket that houses the reports with the read and write data events and log file validation options enabled.
- B. Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled.
- C. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.
- D. Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-cloudtrail-events.html>

Question #254

Topic 1

A business that specializes in online gaming is developing a game that is predicted to be very popular around the globe. A solutions architect must create an AWS Cloud architecture capable of capturing and presenting near-real-time game data for each participant, as well as the names of the world's top 25 players at any one moment.

Which AWS database solution and configuration should be used to satisfy these requirements?

- A. Use Amazon RDS for MySQL as the data store for player activity. Configure the RDS DB instance for Multi-AZ support.
- B. Use Amazon DynamoDB as the data store for player activity. Configure DynamoDB Accelerator (DAX) for the player data.
- C. Use Amazon DynamoDB as the data store for player activity. Configure global tables in each required AWS Region for the player data.
- D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-Region read replicas in each required AWS Region based on player proximity.

Correct Answer: D 

Question #255

Topic 1

A business's application is operating on Amazon EC2 instances contained inside a VPC. One of the apps must make a request to the Amazon S3 API in order to store and retrieve items. The company's security regulations prohibit programs from sending any internet-bound traffic.

Which course of action will satisfy these needs while still maintaining security?

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

Correct Answer: B 

Question #256

Topic 1

A solutions architect is developing a solution that will allow users to browse a collection of photos and make requests for customized images. Parameters for image customisation will be included in each request made to an AWS API Gateway API. The personalized picture will be created on demand, and consumers will get a link to see or download it. The solution must be very user-friendly in terms of viewing and modifying photos.

Which approach is the MOST cost-effective in meeting these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customizations. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customizations. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customizations. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customizations. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Correct Answer: B 

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume – there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service – all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging. All you need to do is supply your code in one of the languages that AWS Lambda supports.

Storing your static content with S3 provides a lot of advantages. But to help optimize your application's performance and security while effectively managing cost, we recommend that you also set up Amazon CloudFront to work with your S3 bucket to serve and protect the content. CloudFront is a content delivery network

(CDN) service that delivers static and dynamic web content, video streams, and APIs around the world, securely and at scale. By design, delivering data out of

CloudFront can be more cost effective than delivering it from S3 directly to your users.

CloudFront serves content through a worldwide network of data centers called Edge Locations. Using edge servers to cache and serve content improves performance by providing content closer to where viewers are located. CloudFront has edge servers in locations all around the world. Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

Question #257

Topic 1

A business runs an Amazon EC2 instance on a private subnet and requires access to a public website in order to get patches and upgrades. The organization does not want other websites to be able to see or start connections to the EC2 instance's IP address.

How can a solutions architect accomplish this goal?

- A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.
- B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.
- C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.
- D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

Correct Answer: B 

Question #258

Topic 1

A business uses AWS to host its website. The website is protected by an Application Load Balancer (ALB) configured to manage HTTP and HTTPS traffic independently.

The firm wishes to route all queries to the website through HTTPS.

What solution should a solutions architect implement to satisfy this criterion?

- A. Update the ALB's network ACL to accept only HTTPS traffic.
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Correct Answer: C 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

Question #259

Topic 1

A business has developed a bespoke application that utilizes embedded credentials to get data from an Amazon RDS MySQL DB instance. According to management, the application's security must be enhanced with the least amount of development work possible.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: D 

Question #260

Topic 1

A solutions architect is developing a system for analyzing financial market performance while the markets are closed. Each night, the system will conduct a succession of compute-intensive operations for four hours. The time required to finish compute tasks is supposed to be constant, and once begun, jobs cannot be stopped. After completion, the system is scheduled to operate for at least one year.

Which Amazon EC2 instance type should be utilized to lower the system's cost?

- A. Spot Instances
- B. On-Demand Instances
- C. Standard Reserved Instances
- D. Scheduled Reserved Instances

Correct Answer: D 

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

Question #261

Topic 1

A business's on-premises data center hosts its critical network services, such as directory services and DNS. AWS Direct Connect connects the data center to the AWS Cloud (DX). Additional AWS accounts are anticipated, which will need continuous, rapid, and cost-effective access to these network services.

What measures should a solutions architect take to ensure that these criteria are met with the LEAST amount of operational overhead possible?

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

Correct Answer: D 

Question #262

Topic 1

A business hosts a multilingual website using a fleet of Amazon EC2 instances protected by an Application Load Balancer (ALB). While this design is presently operational in the us-west-1 Region, it exhibits significant request delay for customers in other regions of the globe. The website must respond fast and effectively to user queries regardless of their location. The organization, however, does not want to duplicate the present infrastructure across numerous Regions.

How is this to be accomplished by a solutions architect?

- A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.
- C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Correct Answer: B 

Question #263

Topic 1

A business is developing a new application for storing a big volume of data. Hourly data analysis and modification will be performed by many Amazon EC2 Linux instances distributed across several Availability Zones. The application team anticipates that the required quantity of space will continue to expand over the following six months.

Which course of action should a solutions architect pursue in order to meet these requirements?

- A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
- B. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
- C. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Correct Answer: B 

Amazon Elastic File System -

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include: big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

Reference:

<https://aws.amazon.com/efs/>

Question #264

Topic 1

A solutions architect is tasked with the responsibility of creating the cloud architecture for a new application that will be hosted on AWS. The process should be parallelized, with the number of jobs to be handled dictating the number of application nodes added and removed. State is not maintained by the processor program. The solutions architect must guarantee that the application is loosely connected and that the task items are kept in a durable manner.

Which design should the architect of solutions use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C 

Amazon Simple Queue Service -

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

Scaling Based on Amazon SQS -

There are some scenarios where you might think about scaling in response to activity in an Amazon SQS queue. For example, suppose that you have a web app that lets users upload images and use them online. In this scenario, each image requires resizing and encoding before it can be published. The app runs on EC2 instances in an Auto Scaling group, and it's configured to handle your typical upload rates. Unhealthy instances are terminated and replaced to maintain current instance levels at all times. The app places the raw bitmap data of the images in an SQS queue for processing. It processes the images and then publishes the processed images where they can be viewed by users. The architecture for this scenario works well if the number of image uploads doesn't vary over time. But if the number of uploads changes over time, you might consider using dynamic scaling to scale the capacity of your Auto Scaling group.

Reference:

<https://aws.amazon.com/sqs/#:~:text=Amazon%20SQS%20leverages%20the%20AWS,queues%20provide%20nearly%20unlimited%20throughput> <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

Question #265

Topic 1

A business is constructing a file-sharing application that will be stored in an Amazon S3 bucket. The firm want to distribute all files using Amazon CloudFront. The firm does not want for the files to be available directly via the S3 URL.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
- C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Correct Answer: C 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/>

Question #266

Topic 1

Numerous business processes inside a corporation need access to data kept in a file share. The file share will be accessed by business systems using the Server Message Block (SMB) protocol. The file sharing solution should be available from both the on-premises and cloud environments of the business.

Which services are required by the business? (Select two.)

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon FSx for Windows
- D. Amazon S3
- E. AWS Storage Gateway file gateway

Correct Answer: CE 

Question #267

Topic 1

A business relies on a traditional on-premises analytics solution that runs on terabytes of.csv files and contains months of data. The older program is unable to cope with the increasing size of.csv files. Daily, new.csv files are uploaded to a common on-premises storage site from numerous data sources. The organization want to maintain support for the traditional application while customers familiarize themselves with AWS analytics capabilities. To do this, the solutions architect want to keep two synchronized copies of all.csv files on-premises and on Amazon S3.

Which solution should the architect of solutions recommend?

- A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company's on-premises storage and the company's S3 bucket.
- B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.
- C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.
- D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon Elastic File System (Amazon EFS) to the company's S3 bucket.

Correct Answer: B 

Question #268

Topic 1

A business is transferring a three-tier application to Amazon Web Services. A MySQL database is required for the program. Previously, application users complained about the program's slow performance while adding new entries. These performance difficulties occurred as a result of users creating various real-time reports from the program during business hours.

Which solution will optimize the application's performance when it is migrated to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Correct Answer: C **Amazon RDS Read Replicas Now Support Multi-AZ Deployments**

Starting today, Amazon RDS Read Replicas for MySQL and MariaDB now support Multi-AZ deployments. Combining Read Replicas with Multi-AZ enables you to build a resilient disaster recovery strategy and simplify your database engine upgrade process.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS

Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

You can also combine Read Replicas with Multi-AZ for your database engine upgrade process. You can create a Read Replica of your production database instance and upgrade it to a new database engine version. When the upgrade is complete, you can stop applications, promote the Read Replica to a standalone database instance, and switch over your applications. Since the database instance is already a Multi-AZ deployment, no additional steps are needed.

Overview of Amazon RDS Read Replicas

Deploying one or more read replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more read replicas.

Serving read traffic while the source DB instance is unavailable. In some cases, your source DB instance might not be able to take I/O requests, for example due to I/O suspension for backups or scheduled maintenance. In these cases, you can direct read traffic to your read replicas. For this use case, keep in mind that the data on the read replica might be "stale" because the source DB instance is unavailable.

Business reporting or data warehousing scenarios where you might want business reporting queries to run against a read replica, rather than your primary, production DB instance.

Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the source DB instance fails.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #269

Topic 1

A business has an AWS account for software engineering purposes. Through a pair of AWS Direct Connect connections, the AWS account gets access to the company's on-premises data center. All traffic that does not originate in a virtual private cloud is routed via the virtual private gateway.

A development team recently used the console to construct an AWS Lambda function. The development team must provide access to a database that is located on a private subnet in the company's data center.

Which solution will satisfy these criteria?

- A. Configure the Lambda function to run in the VPC with the appropriate security group.
- B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
- C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
- D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>

Question #270

Topic 1

A corporation has an on-premises MySQL database that is used infrequently by the worldwide sales staff. The sales team needs little database downtime. A database administrator wishes to move this database to AWS without specifying an instance type in front of increased user traffic in the future.

Which solution architect service should be recommended?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

Correct Answer: A 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/migrate-mysql-rds-dms/>

Question #271

Topic 1

A corporation is developing an architecture for a mobile application that needs the least amount of delay possible for its consumers. The company's architecture is comprised of Amazon EC2 instances that are routed via an Application Load Balancer that is configured to operate in an Auto Scaling group. Amazon EC2 instances communicate with Amazon RDS. Beta testing of the application revealed a slowness while reading the data. However, the data suggest that no CPU usage criteria are exceeded by the EC2 instances.

How can this problem be resolved?

- A. Reduce the threshold for CPU utilization in the Auto Scaling group.
- B. Replace the Application Load Balancer with a Network Load Balancer.
- C. Add read replicas for the RDS instances and direct read traffic to the replica.
- D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

Correct Answer: C 

Question #272

Topic 1

A business's application architecture is two-tiered and distributed over public and private subnets. The public subnet contains Amazon EC2 instances that execute the web application, whereas the private subnet has a database. The web application instances and database are both contained inside a single Availability Zone (AZ).

Which combination of measures should a solutions architect take to ensure this architecture's high availability? (Select two.)

- A. Create new public and private subnets in the same AZ for high availability.
- B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.
- C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.
- D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.
- E. Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Correct Answer: BE 

Question #273

Topic 1

A business want to utilize Amazon S3 as a supplementary storage location for its on-premises dataset. The business would seldom need access to this copy. The cost of the storage solution should be kept to a minimum.

Which storage option satisfies these criteria?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: D 

Question #274

Topic 1

A business has an application with a REST-based interface that enables near-real-time data retrieval from a third-party vendor. After receiving the data, the program analyzes and saves it for further analysis. Amazon EC2 instances are used to host the application. When delivering data to the program, the third-party vendor saw many 503 Service Unavailable errors. When data volume increases, the compute capacity approaches its limit and the application becomes unable of processing all requests.

Which design should a solutions architect advocate in order to achieve more scalability?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A 

Question #275

Topic 1

A business has developed an application that analyzes inventory data by using overnight digital photographs of items on shop shelves. The application is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB) and retrieves photos from an Amazon S3 bucket for metadata processing by worker nodes. A solutions architect must guarantee that worker nodes process each picture.

What actions should the solutions architect take to ensure that this need is met in the MOST cost-effective manner possible?

- A. Send the image metadata from the application directly to a second ALB for the worker nodes that use an Auto Scaling group of EC2 Spot Instances as the target group.
- B. Process the image metadata by sending it directly to EC2 Reserved Instances in an Auto Scaling group. With a dynamic scaling policy, use an Amazon CloudWatch metric for average CPU utilization of the Auto Scaling group as soon as the front-end application obtains the images.
- C. Write messages to Amazon Simple Queue Service (Amazon SQS) when the front-end application obtains an image. Process the images with EC2 On-Demand instances in an Auto Scaling group with instance scale-in protection and a fixed number of instances with periodic health checks.
- D. Write messages to Amazon Simple Queue Service (Amazon SQS) when the application obtains an image. Process the images with EC2 Spot Instances in an Auto Scaling group with instance scale-in protection and a dynamic scaling policy using a custom Amazon CloudWatch metric for the current number of messages in the queue.

Correct Answer: B 

Question #276

Topic 1

In the us-east-1 Region, a corporation has three VPCs designated Development, Testing, and Production. The three virtual private clouds must be linked to an on-premises data center and are meant to be self-contained in order to ensure security and avoid resource sharing. A solutions architect must identify a solution that is both scalable and safe.

What recommendations should the solutions architect make?

- A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.
- B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.
- C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.
- D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

Correct Answer: B 

Question #277

Topic 1

A business may have several projects running in various AWS Regions. Typically, the projects have a three-tier architecture comprised of Amazon EC2 instances that are routed via an Application Load Balancer. The instances are managed as part of an Auto Scaling group and share Amazon Elastic File System (Amazon EFS) storage and Amazon Relational Database Service (Amazon RDS) databases. Certain initiatives need resources from many regions. A solutions architect must determine the expenses associated with each project.

Which method requires the LEAST amount of operational effort to convey this information?

- A. Use Cost Explorer to perform one-time queries for each Region and create a report that filters by project.
- B. Use the AWS Billing and Cost Management details page to see the actual usage costs of the resources by project.
- C. Use AWS Systems Manager to group resources by project and monitor each project's resources and cost.
- D. Use AWS Billing and Cost Management to activate cost allocation tags and create reports that are based on the project tags.

Correct Answer: D 

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>

Question #278

Topic 1

A business has retained the services of a solutions architect to develop a dependable architecture for its application. The application is comprised of a single Amazon RDS database instance and two manually deployed Amazon EC2 instances running web servers. A single Availability Zone contains all of the EC2 instances.

An employee recently removed the database instance, resulting in the application being offline for 24 hours. The firm is concerned with the environment's general dependability.

What should the solutions architect do to ensure the application's infrastructure is as reliable as possible?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Correct Answer: D 

Question #279

Topic 1

A business operates an application on an Amazon EC2 instance using Amazon Elastic Block Store as a backend (Amazon EBS). The instance must be accessible for a minimum of 12 hours every day. The corporation want to save money by making the instance inaccessible outside of the application's window. However, when the instance is inaccessible, the contents of its memory must be maintained.

What actions should a solutions architect do in order to satisfy this requirement?

- A. Stop the instance outside the application's availability window. Start up the instance again when required.
- B. Hibernate the instance outside the application's availability window. Start up the instance again when required.
- C. Use Auto Scaling to scale down the instance outside the application's availability window. Scale up the instance when required.
- D. Terminate the instance outside the application's availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

Correct Answer: B 

Question #280

Topic 1

What steps should a solutions architect take to assure the encryption of all items submitted to an Amazon S3 bucket?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

Correct Answer: D 

Question #281

Topic 1

A manufacturing business is interested in implementing predictive maintenance on its machines. The business will deploy hundreds of IoT sensors that will transmit real-time data to AWS. A solutions architect is entrusted with the responsibility of designing a solution that will receive events in an orderly fashion for each piece of equipment and will guarantee that data is preserved for subsequent processing.

Which option is the MOST EFFECTIVE?

- A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.
- B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon Elastic Block Store (Amazon EBS).
- C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon Elastic File System (Amazon EFS).
- D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

Correct Answer: D 

Question #282

Topic 1

A solutions architect is tasked with the responsibility of developing a customer-facing application. The application is projected to have a varying number of reads and writes throughout the year, with well defined access patterns. Database auditing and scalability must be controlled in the AWS Cloud. The Recovery Point Objective (RPO) cannot exceed five hours.

Which solutions are capable of doing this? (Select two.)

- A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
- B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
- C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
- D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
- E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

Correct Answer: AB 

Question #283

Topic 1

A business is launching an application that batch processes massive amounts of data as required. The workload will be run on Amazon EC2 instances. The network design must be extremely scalable and avoid groupings of nodes having the same underlying hardware.

Which network solution combination will suit these requirements? (Select two.)

- A. Create Capacity Reservations for the EC2 instances to run in a placement group.
- B. Run the EC2 instances in a spread placement group.
- C. Run the EC2 instances in a cluster placement group.
- D. Place the EC2 instances in an EC2 Auto Scaling group.
- E. Run the EC2 instances in a partition placement group.

Correct Answer: BC 

Reference:

<https://ipwitthease.com/ec2-placement-groups-aws/>

Question #284

Topic 1

A security team that is responsible for restricting access to certain services or activities across all of the team's AWS accounts. All accounts in AWS Organizations are part of a huge organization.

The solution must be scalable, and permissions must be managed centrally.

What actions should a solutions architect take to achieve this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Correct Answer: D 

Service Control Policy concepts -

SCPs offer central access controls for all IAM entities in your accounts. You can use them to enforce the permissions you want everyone in your business to follow. Using SCPs, you can give your developers more freedom to manage their own permissions because they can only operate within the boundaries you define.

You create and apply SCPs through AWS Organizations. When you create an organization, AWS Organizations automatically creates a root, which forms the parent container for all the accounts in your organization. Inside the root, you can group accounts in your organization into organizational units (OUs) to simplify management of these accounts. You can create multiple OUs within a single organization, and you can create OUs within other OUs to form a hierarchical structure. You can attach SCPs to the organization root, OUs, and individual accounts. SCPs attached to the root and OUs apply to all OUs and accounts inside of them.

SCPs use the AWS Identity and Access Management (IAM) policy language; however, they do not grant permissions. SCPs enable you set permission guardrails by defining the maximum available permissions for IAM entities in an account. If a SCP denies an action for an account, none of the entities in the account can take that action, even if their IAM permissions allow them to do so. The guardrails set in SCPs apply to all

IAM entities in the account, which include all users, roles, and the account root user.

Reference:

<https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-aws-organization/>

#~:text=Central%20security%20administrators%20use%20service,users%20and%20roles)%20adhere%20to.&text=Now%2C%20using%20SCPs%2C%20you%

20can,your%20organization%20or%20organizational%20unit

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Question #285

Topic 1

Recently, we transferred a monolithic application to AWS and it is currently operating on a single Amazon EC2 machine. Due to application limits, automated scaling cannot be used to scale out the application. The chief technology officer (CTO) desires an automated method for restoring the EC2 instance in the very improbable event that the underlying hardware breaks.

What would enable the quickest feasible automated recovery of the EC2 instance?

- A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.
- B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.
- C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.
- D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

Correct Answer: A 

Question #286

Topic 1

Internally, a business must communicate media and application files. At the moment, users are authorized through Active Directory and have access to files via a Microsoft Windows platform. The chief executive officer wants to maintain the same user rights as before, but wishes for the corporation to enhance the procedure as it nears its storage capacity limit.

What recommendations should a solutions architect make?

- A. Set up a corporate Amazon S3 bucket and move all media and application files.
- B. Configure Amazon FSx for Windows File Server and move all the media and application files.
- C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.
- D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

Correct Answer: B 

Reference:

<https://aws.amazon.com/fsx/windows/>

Question #287

Topic 1

A business wants to share data from self-driving vehicles with the broader automotive community. The data will be accessed through an Amazon S3 bucket. The organization want to keep the expense of making this data accessible to other AWS customers to a minimum.

What actions should a solutions architect take to achieve this objective?

- A. Create an S3 VPC endpoint for the bucket.
- B. Configure the S3 bucket to be a Requester Pays bucket.
- C. Create an Amazon CloudFront distribution in front of the S3 bucket.
- D. Require that the files be accessible only with the use of the BitTorrent protocol.

Correct Answer: B 

You can configure an Amazon S3 bucket to be a Requester Pays bucket so that the requester pays the cost of the request and data download instead of the bucket owner.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysExamples.html>

Question #288

Topic 1

A business utilizes an AWS Lambda function to retrieve and decrypt data from Amazon S3. These files are encrypted using Customer Master Keys for AWS Key Management Service (AWS KMS CMKs). A solutions architect must create a solution that properly sets the needed permissions.

Which action combination does this? (Select two.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy.
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy.
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Correct Answer: BE 

Question #289

Topic 1

A business operates a Microsoft.NET application on an on-premises Windows Server. The program makes use of an Oracle Database Standard Edition server to store data. The firm is in the process of migrating to AWS and want to minimize development modifications throughout the process. The Amazon Web Services application environment should be very reliable.

Which steps should the organization take in combination to achieve these requirements? (Select two.)

- A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Correct Answer: BD 

The .NET web application is deployed to AWS Elastic Beanstalk, which runs in an Amazon EC2 Auto Scaling Group. You can set up a scaling policy based on

Amazon CloudWatch metrics such as CPU utilization. For a database, you can use Amazon RDS in a Multi-AZ environment.

Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-a-net-application-from-microsoft-azure-app-service-to-aws-elastic-beanstalk.html> <https://aws.amazon.com/dms/>

Question #290

Topic 1

A business experiences uneven service from its data center supplier as a result of its location in a natural disaster-prone region. Although the organization is not ready to completely move to the AWS Cloud, it does desire a failover scenario on AWS in the event that the on-premises data center fails.

The business operates web servers that link to third-party providers. The data stored on AWS and on-premises must be consistent.

Which solution, according to a solutions architect, should have the LEAST amount of downtime?

- A. Configure an Amazon Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.
- C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.
- D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

Correct Answer: A 

Question #291

Topic 1

A solutions architect is developing an application that will handle large-scale batch processing of data. Amazon S3 will be used to store the input data, while another S3 bucket will be used to keep the output data. The program will handle the data by transferring it over the network across different Amazon EC2 instances.

What should the solutions architect do to minimize the total cost of data transfer?

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

Correct Answer: B 

Question #292

Topic 1

A packaged application created and returned by a business dynamically produces and returns single-use text files in response to user requests. The firm is already distributing content using Amazon CloudFront, but wants to further minimize data transmission costs. The firm is not permitted to edit the source code of the program.

What actions should a solutions architect do to save money?

- A. Use Lambda@Edge to compress the files as they are sent to users.
- B. Enable Amazon S3 Transfer Acceleration to reduce the response times.
- C. Enable caching on the CloudFront distribution to store generated files at the edge.
- D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

Correct Answer: A 

Question #293

Topic 1

A business that now maintains a website on-premises want to move it to the AWS Cloud. Although the website exposes a single hostname to the internet, it routes its functionalities to distinct on-premises server groups dependent on the URL path. The server groups are individually scaled in accordance with the requirements of the services they support. The company's on-premises network is connected through an AWS Direct Connect link.

What should a solutions architect do to ensure that traffic is sent to the proper set of servers using path-based routing?

- A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.
- B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.
- C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.
- D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer for the group of servers supporting that path.

Correct Answer: B 

Question #294

Topic 1

A business collects organized clickstream data from numerous websites and analyzes it using batch processing. Each day, the firm gets 100 million event records, each of which is around 1 KB in size. Each night, the organization imports data onto Amazon Redshift, which business analysts ingest.

The organization wishes to transition to near-real-time data processing in order to provide timely insights. The solution should process the streaming data with the least amount of operational overhead as feasible.

Which AWS service combination best meets these objectives in terms of cost-effectiveness? (Select two.)

- A. Amazon EC2
- B. AWS Batch
- C. Amazon Simple Queue Service (Amazon SQS)
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Correct Answer: CE 

Question #295

Topic 1

The website of a business, which is hosted on Amazon EC2 instances, handles classified data that is stored in Amazon S3. The organization wants a private and secure connection between its EC2 resources and Amazon S3 due to security concerns.

Which solution satisfies these criteria?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html>

Question #296

Topic 1

A solutions architect is developing a new virtual private cloud (VPC) architecture. Two public subnets are reserved for the load balancer, two private subnets are reserved for web servers, and two private subnets are reserved for MySQL. HTTPS is the sole protocol used by the web servers. The solutions architect has previously configured the load balancer's security group to enable access to port 443 from 0.0.0.0/0. According to company policy, each resource must have the least amount of access necessary to accomplish its functions.

Which extra configuration technique should the solutions architect do in order to satisfy these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Correct Answer: C 

Question #297

Topic 1

A business is evaluating various options for collecting, processing, and storing data about how people utilize their services. The business aim is to provide an analytics capability that enables the organization to easily acquire operational insights using regular SQL queries. The solution should be highly accessible and adhere to the data tier's Atomicity, Consistency, Isolation, and Durability (ACID) requirements.

Which solution, if any, should a solutions architect suggest?

- A. Use an Amazon Timestream database.
- B. Use an Amazon Neptune database in a Multi-AZ design.
- C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.
- D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS) Throughput Optimized HDD (st1) storage.

Correct Answer: C 

Question #298

Topic 1

A business stores its static website content in the us-east-1 Region through an Amazon S3 bucket. The bucket's content is made accessible through an Amazon CloudFront origin pointing to it. Cross-Region replication is enabled, which will replicate the bucket to the ap-southeast-1 Region. The management team is looking for a solution that would increase the website's availability.

Which activities should a solutions architect perform in conjunction to enhance availability? (Select two.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53.
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Correct Answer: BE 

Question #299

Topic 1

A business transferred a two-tier application from its on-premises data center to the Amazon Web Services Cloud. The data layer is a multi-AZ Amazon RDS for Oracle configuration with 12' of Amazon Elastic Block Store (Amazon EBS) general purpose SSD storage. The program is intended to process and store documents as binary big objects (blobs) with an average document size of 6 MB in the database.

The database has increased in size over time, lowering performance and increasing storage costs. The organization wants to boost database performance and need a highly available and robust solution.

Which approach will be the most cost-effective in meeting these requirements?

- A. Reduce the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Magnetic.
- B. Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.
- C. Create an Amazon S3 bucket. Update the application to store documents in the S3 bucket. Store the object metadata in the existing database.
- D. Create an Amazon DynamoDB table. Update the application to use DynamoDB. Use AWS Database Migration Service (AWS DMS) to migrate data from the Oracle database to DynamoDB.

Correct Answer: D 

Reference:

<https://aws.amazon.com/getting-started/hands-on/break-free-from-legacy-databases/migrate-sql-server-to-amazon-dynamodb/>

Question #300

Topic 1

A business has just expanded worldwide and want to make its application available to consumers in those new markets. The application is deployed on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The firm need the capacity to redirect traffic from one region's resources to another.

What recommendations should a solutions architect make?

- A. Configure an Amazon Route 53 latency routing policy.
- B. Configure an Amazon Route 53 geolocation routing policy.
- C. Configure an Amazon Route 53 geoproximity routing policy.
- D. Configure an Amazon Route 53 multivalue answer routing policy.

Correct Answer: C 

Question #301

Topic 1

A business must consume and manage massive volumes of streaming data generated by its application. The application is deployed on Amazon EC2 instances and communicates with Amazon Kinesis Data Streams, which is setup with default parameters. The application consumes and publishes data to an Amazon S3 bucket every other day for business intelligence (BI) analysis. The business notes that Amazon S3 is not getting all of the data sent to Kinesis Data Streams by the application.

What is the best course of action for a solutions architect to take in order to tackle this issue?

- A. Update the Kinesis Data Streams default settings by modifying the data retention period.
- B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Correct Answer: C 

Reference:

<https://aws.amazon.com/kinesis/data-firehose/faqs/>

Question #302

Topic 1

A business is developing a web application on AWS for the purpose of processing insurance quotations. The program will allow users to seek quotations. Quotes must be classified according to quotation type and must be answered to within 24 hours or risk being lost. The solution should be straightforward to implement and maintain.

Which solution satisfies these criteria?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).
- B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

Correct Answer: D 

Question #303

Topic 1

A business is developing a new application that will operate in a virtual private cloud on Amazon EC2 instances. The program stores data in Amazon S3 and accesses it using Amazon DynamoDB. The corporation forbids any communication between EC2 instances and other AWS services from traveling over the public internet for compliance concerns.

What can a solution architect do to satisfy this criterion?

- A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB.
- B. Configure interface VPC endpoints to Amazon S3 and DynamoDB.
- C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.
- D. Configure a gateway VPC endpoint to DynamoDB. Configure an interface VPC endpoint to Amazon S3.

Correct Answer: C 

Question #304

Topic 1

A business has created a new AWS account. The account is freshly established, and no changes to the default settings have been made. The organization is worried about the AWS account root user's security.

What measures should be taken to safeguard the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

Correct Answer: B 

Question #305

Topic 1

An organization hosts an application on Amazon EC2 instances on two private subnets. A solutions architect's goal is to make the application as easily accessible as possible over the public internet.

What recommendations should the solutions architect make?

- A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.
- C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.
- D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two private subnets from the same Availability Zones as the public instances.

Correct Answer: C 

Question #306

Topic 1

A business is ingesting data from on-premises data sources utilizing a fleet of Amazon EC2 instances. The data is in JSON format and may be ingested at a rate of up to 1 MB/s. When an EC2 instance is restarted, any data that was in transit is lost. The data science team at the organization want to query ingested data in near-real time.

Which method enables near-real-time data querying while being scalable and causing the least amount of data loss?

- A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

Correct Answer: A 

Question #307

Topic 1

On AWS, a business is operating a multi-tier web application. The application's database layer is powered by Amazon Aurora MySQL. The application and database layers are located in the region us-east-1. A database administrator who checks the Aurora DB cluster on a regular basis notices that an occasional surge in read traffic results in high CPU use on the read replica, increasing the application's read latency.

What should a solutions architect do to increase the read scalability of their application?

- A. Reboot the Aurora DB cluster.
- B. Create a cross-Region read replica
- C. Increase the instance class of the read replica.
- D. Configure Aurora Auto Scaling for the read replica.

Correct Answer: D 

Question #308

Topic 1

A business has a number of apps that make use of Amazon RDS for MySQL as the database. Recently, the organization realized that a new custom reporting application had increased the database's query count. This results in a decrease in performance.

How could a solutions architect address this problem with the fewest number of application modifications possible?

- A. Add a secondary DB instance using Multi-AZ.
- B. Set up a read replica and Multi-AZ on Amazon RDS.
- C. Set up a standby replica and Multi-AZ on Amazon RDS.
- D. Use caching on Amazon RDS to improve the overall performance.

Correct Answer: D 

Question #309

Topic 1

A firm is developing a web application on AWS utilizing containers. At any one moment, the organization needs three instances of the web application to be running. The application must be scalable in order to keep up with demand increases. While management is cost-conscious, they agree that the application should be highly accessible.

What recommendations should a solutions architect make?

- A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

Correct Answer: D 

Question #310

Topic 1

A business needs a resilient backup storage solution for its on-premises database servers, while also guaranteeing that on-premises apps have access to these backups for rapid recovery. The corporation will store these backups on AWS storage services. A solutions architect is responsible for developing a solution with the least amount of operational overhead possible.

Which solution should be implemented by the solutions architect?

- A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.
- B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.
- C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.
- D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

Correct Answer: A 

Question #311

Topic 1

AWS Organizations enables a business to manage many AWS accounts for various departments. The management account has an Amazon S3 bucket where project reports are stored. The corporation wishes to restrict access to this S3 bucket to people with AWS Organizations accounts.

Which method satisfies these criteria with the FEASTEST operational overhead?

- A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
- C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
- D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Correct Answer: D 

Question #312

Topic 1

A business intends to utilize Amazon S3 to store sensitive user data. Internal security compliance requirements demand that data be encrypted prior to being sent to Amazon S3.

What recommendations should a solutions architect make to meet these requirements?

- A. Server-side encryption with customer-provided encryption keys
- B. Client-side encryption with Amazon S3 managed encryption keys
- C. Server-side encryption with keys stored in AWS Key Management Service (AWS KMS)
- D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

Correct Answer: D 

Question #313

Topic 1

A business has developed a bespoke application that runs on an Amazon EC2 instance and performs the following functions:

- * Reads a large amount of data from Amazon S3
- * Performs a multi-stage analysis
- * Writes the results to Amazon DynamoDB

During the multi-stage analysis, the program creates a huge number of big temporary files. The performance of the procedure is dependent on the performance of the temporary storage.

What would be the quickest method of storing temporary files?

- A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.
- B. Multiple Amazon Elastic Block Store (Amazon EBS) drives with Provisioned IOPS and EBS optimization.
- C. Multiple Amazon Elastic File System (Amazon EFS) volumes using the Network File System version 4.1 (NFSv4.1) protocol.
- D. Multiple instance store volumes with software RAID 0.

Correct Answer: A 

Question #314

Topic 1

A solutions architect is tasked with the responsibility of designing a database solution for a high-volume ecommerce online application. Customer profiles and shopping cart information are stored in the database. The database must be able to handle several million queries per second at its peak and respond in milliseconds. The operational overhead associated with database aging and scalability must be kept to a minimum.

Which database solution should be recommended by the solutions architect?

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

Correct Answer: A 

Question #315

Topic 1

For security concerns, a business has many Amazon EC2 instances configured in a private subnet. These instances are used to run applications that frequently read and write huge volumes of data to and from Amazon S3. At the moment, subnet routing routes all traffic to the internet via a NAT gateway. The organization wishes to reduce overall costs while maintaining the application's capacity to interface with Amazon S3 or the public internet.

What actions should a solutions architect do to save costs?

- A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.
- B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.
- C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.
- D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

Correct Answer: C 

Question #316

Topic 1

A business is developing a new web application that will be deployed in a single AWS Region. A two-tier design is required for the application, which will use Amazon EC2 instances and an Amazon RDS database instance. A solutions architect must plan the application's architecture in such a way that all components are highly accessible.

Which approach will be the most cost-effective in meeting these requirements?

- A. Deploy EC2 instances in an additional Region. Create a DB instance with the Multi-AZ option activated.
- B. Deploy all EC2 instances in the same Region and the same Availability Zone. Create a DB instance with the Multi-AZ option activated.
- C. Deploy EC2 instances across at least two Availability Zones within the same Region. Create a DB instance in a single Availability Zone.
- D. Deploy EC2 instances across at least two Availability Zones within the same Region. Create a DB instance with the Multi-AZ option activated.

Correct Answer: C 

Question #317

Topic 1

On-premises, a business has a sizable Microsoft SharePoint implementation that needs Microsoft Windows shared file storage. The organization is contemplating migrating this workload to AWS Cloud and evaluating other storage solutions. The storage solution must be highly available and have access control coupled with Active Directory.

Which solution will meet these criteria?

- A. Configure Amazon EFS Amazon Elastic File System (Amazon EFS) storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Correct Answer: D 

Reference:

<https://aws.amazon.com/fsx/windows/>

Question #318

Topic 1

The website of a business is hosted on Amazon EC2 instances protected by an Application Load Balancer (ALB). There is a combination of dynamic and static information on the website. Users from all around the world are complaining about the website's slowness.

Which set of activities will result in an increase in website performance for global users?

- A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
- C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross-Region VPC peering.
- D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

Correct Answer: A 

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Routing traffic to an Amazon CloudFront web distribution by using your domain name.

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website — including dynamic, static, streaming, and interactive content — by using a global network of edge locations.

Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

To use CloudFront to distribute your content, you create a web distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want

CloudFront to get your content from, whether you want only selected users to have access to your content, and whether you want to require users to use HTTPS.

When you create a web distribution, CloudFront assigns a domain name to the distribution, such as `asd11111abcdef8.cloudfront.net`. You can use this domain name in the URLs for your content, for example:

[1]

Alternatively, you might prefer to use your own domain name in URLs, for example:

[1]

If you want to use your own domain name, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. An alias record is a Route

53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as `example.com`, and for subdomains, such as `www.example.com`. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #319

Topic 1

A firm uses the AWS Cloud to host its multi-tiered public web application. Amazon EC2 instances host the web application, while Amazon RDS hosts the database. The firm anticipates a significant boost in revenues during the forthcoming holiday weekend. A solutions architect must provide a solution for analyzing the web application's performance with a granularity of no more than two minutes.

What actions should the solutions architect do in order to satisfy this requirement?

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

Correct Answer: B 

Question #320

Topic 1

A corporation uses AWS to host its product information websites. The present approach deploys numerous Amazon C2 instances in an Auto Scaling group behind an Application Load Balancer. Additionally, the website utilizes a special DNS name and interacts over HTTPS only using a dedicated SSL certificate. The firm is in the process of launching a new product and wants to ensure that people from all over the globe enjoy the greatest experience possible on the new website.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Correct Answer: A 

What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

If the content is not in that edge location, CloudFront retrieves it from an origin that you've defined — such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

As an example, suppose that you're serving an image from a traditional web server, not from CloudFront. For example, you might serve an image,

[1]

Your users can easily navigate to this URL and see the image. But they probably don't know that their request was routed from one network to another — through the complex collection of interconnected networks that comprise the internet — until the image was found.

CloudFront speeds up the distribution of your content by routing each user request through the AWS backbone network to the edge location that can best serve your content. Typically, this is a CloudFront edge server that provides the fastest delivery to the viewer. Using the AWS network dramatically reduces the number of networks that your users' requests must pass through, which improves performance. Users get lower latency — the time it takes to load the first byte of the file — and higher data transfer rates.

You also get increased reliability and availability because copies of your files (also known as objects) are now held (or cached) in multiple edge locations around the world.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Question #321

Topic 1

A business has an application that stores data in Amazon Elastic File System (Amazon EFS). The files are 1 GB or bigger in size and are often visited during the first several days after production. The data for the application is distributed over a cluster of Linux servers. The corporation wishes to lower the application's storage expenses.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Implement Amazon FSx and mount the network drive on each server.
- B. Move the files from Amazon Elastic File System (Amazon EFS) and store them locally on each Amazon EC2 instance.
- C. Configure a Lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.
- D. Move the files to Amazon S3 with S3 lifecycle policies enabled. Rewrite the application to support mounting the S3 bucket.

Correct Answer: C 

Question #322

Topic 1

Recently, a business moved a message processing system to AWS. The system accepts messages into an Amazon EC2 instance's ActiveMQ queue. A consumer application running on Amazon EC2 processes the messages. The consumer application processes the messages and writes the results to an Amazon EC2 MySQL database. The organization wants a highly accessible application with little operational complexity.

Which architecture is the MOST RELIABLE?

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

Correct Answer: D 

Question #323

Topic 1

Recently, a corporation created its website in order to deliver information to its worldwide user base. The firm wishes to store and speed the delivery of static material to its consumers via the usage of Amazon CloudFront and an Amazon EC2 instance as the origin.

How should a solutions architect maximize an application's high availability?

- A. Use Lambda@Edge for CloudFront.
- B. Use Amazon S3 Transfer Acceleration for CloudFront.
- C. Configure another EC2 instance in a different Availability Zone as part of the origin group.
- D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

Correct Answer: A 

Question #324

Topic 1

AWS-hosted application is having performance issues, and the application vendor want to analyze the log file in order to troubleshoot further. The log file is 10 GB in size and is hosted on Amazon S3. For a short period, the application owner will make the log file accessible to the vendor.

What is the MOST SECURE method of doing this?

- A. Enable public read on the S3 object and provide the link to the vendor.
- B. Upload the file to Amazon WorkDocs and share the public link with the vendor.
- C. Generate a presigned URL and have the vendor download the log file before it expires.
- D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Correct Answer: C 

Share an object with others -

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects. When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method

(GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.

Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

Question #325

Topic 1

A solutions architect is tasked with the responsibility of building a two-tier online application. The application is composed of a front-end web layer that is hosted on Amazon EC2 on public subnets. The database layer is comprised of Microsoft SQL Server instances operating in a private subnet on Amazon EC2. The organization places a high premium on security.

In this case, how should security groups be configured? (Select two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: AC 

Question #326

Topic 1

A ride-hailing company's historical data on service consumption is organized. Amazon S3 csv data files A data analyst must run SQL queries on this data.

A solutions architect must offer a solution that maximizes the query's cost-effectiveness.

Which solution satisfies these criteria?

- A. Create an Amazon EMR cluster. Load the data. Perform the queries.
- B. Create an Amazon Redshift cluster. Import the data. Perform the queries.
- C. Create an Amazon Aurora PostgreSQL DB cluster. Import the data. Perform the queries.
- D. Create an Amazon Athena database. Associate the data in Amazon S3. Perform the queries.

Correct Answer: D 

Reference:

<https://searchcloudcomputing.techtarget.com/answer/Compare-EMR-Redshift-and-Athena-for-data-analysis-on-AWS>

Question #327

Topic 1

The website of a business is served by an Auto Scaling group of Amazon EC2 instances in a single AWS Region. A database is not required for the website.

The firm is growing, and the technical staff of the company distributes the website to a second Region. The firm want to spread traffic across the two Regions in order to allow expansion and catastrophe recovery. The solution should avoid serving visitors from regions where the website is infected.

Which policy or resource should the business implement in order to comply with these requirements?

- A. An Amazon Route 53 simple routing policy
- B. An Amazon Route 53 multivalue answer routing policy
- C. An Application Load Balancer in one Region with a target group that specifies the EC2 instance IDs from both Regions
- D. An Application Load Balancer in one Region with a target group that specifies the IP addresses of the EC2 instances from both Regions

Correct Answer: B 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>

Question #328

Topic 1

A solutions architect is tasked with the responsibility of developing a new Amazon CloudFront distribution for an application. Certain information given by users is considered sensitive. Although the program employs HTTPS, it requires an additional layer of protection. Sensitive data should be safeguarded throughout the whole application stack, and access to it should be limited to specific apps.

Which course of action should be taken by the solutions architect?

- A. Configure a CloudFront signed URL
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

Correct Answer: A 

Question #329

Topic 1

A web application is hosted on Amazon EC2 instances, which are routed through an Application Load Balancer. Users may construct bespoke reports using historical weather data. A report may take up to five minutes to generate. These lengthy queries use a significant portion of the system's available incoming connections, rendering the system unusable to other users.

How can a solutions architect increase the responsiveness of a system?

- A. Use Amazon SQS with AWS Lambda to generate reports.
- B. Increase the idle timeout on the Application Load Balancer to 5 minutes.
- C. Update the client-side application code to increase its request timeout to 5 minutes.
- D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

Correct Answer: A 

Question #330

Topic 1

A business currently maintains a static website on-premises and want to transfer it to AWS. For visitors worldwide, the website should load as rapidly as possible. Additionally, the business seeks the most cost-effective option.

What actions should a solutions architect take to achieve this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
- D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Correct Answer: B **What Is Amazon CloudFront?**

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users.

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with

CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #331

Topic 1

A business has developed an application that analyzes millions of connected devices for security concerns and records the results to an Amazon S3 bucket. Each week, the organization generates around 70 GB of data, and the corporation must retain three years of data for historical reporting. The organization must analyze, aggregate, and enhance data from Amazon S3 in the shortest period of time possible by conducting complicated analytical queries and joins. On an Amazon QuickSight dashboard, the aggregated dataset is shown.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Create and run an ETL job in AWS Glue to process the data from Amazon S3 and load it into Amazon Redshift. Perform the aggregation queries on Amazon Redshift.
- B. Use AWS Lambda functions based on S3 PutObject event triggers to copy the incremental changes to Amazon DynamoDB. Perform the aggregation queries on DynamoDB.
- C. Use AWS Lambda functions based on S3 PutObject event triggers to copy the incremental changes to Amazon Aurora MySQL. Perform the aggregation queries on Aurora MySQL.
- D. Use AWS Glue to catalog the data in Amazon S3. Perform the aggregation queries on the cataloged tables by using Amazon Athena. Query the data directly from Amazon S3.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/build-an-etl-service-pipeline-to-load-data-incrementally-from-amazon-s3-to-amazon-redshift-using-aws-glue.html>

Question #332

Topic 1

A firm runs many business apps in three distinct virtual private clouds (VPCs) inside the eu-east-1 Region. Applications must be able to interact with one another across VPCs. Additionally, the apps must be capable of sending hundreds of terabytes of data daily to a latency-sensitive application running in a single on-premises data center.

A solutions architect's primary responsibility is to build a network connection solution that is as cost-effective as possible.

Which solution satisfies these criteria?

- A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
- B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
- D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

Question #333

Topic 1

Each day at 12:00, a website hosts a web application that gets a spike of traffic. Daily, people submit fresh images and material, but have complained about timeouts. The design makes advantage of Amazon EC2 Auto Scaling groups, and the custom application takes an average of one minute to start up before responding to user queries.

How should a solutions architect reimagine the architecture in order to adapt to shifting traffic patterns?

- A. Configure a Network Load Balancer with a slow start configuration.
- B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.
- C. Configure an Auto Scaling step scaling policy with an instance warmup condition.
- D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

Correct Answer: D 

Question #334

Topic 1

A corporation has implemented a new auditing system to consolidate information about Amazon EC2 instance operating system versions, patching, and installed applications. A solutions architect must guarantee that all instances provisioned through EC2 Auto Scaling groups correctly deliver audit reports to the auditing system at startup and shutdown.

Which method accomplishes these objectives the MOST EFFECTIVELY?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

Correct Answer: B 

Question #335

Topic 1

A solutions architect is developing a new hybrid architecture to migrate an organization's on-premises infrastructure to Amazon Web Services. The organization seeks a highly accessible connection to an AWS Region with constant low latency. The firm is concerned with cost containment and is ready to endure slower traffic in the event that the main connection breaks.

What actions should the solutions architect take to ensure that these criteria are met?

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

Correct Answer: C 

Question #336

Topic 1

A business is transferring a cluster of NoSQL databases to Amazon EC2. The database duplicates data automatically in order to retain at least three copies of it. The servers' I/O throughput is of the utmost importance.

What sort of instance should a solutions architect propose for the migration?

- A. Storage optimized instances with instance store
- B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume
- C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled
- D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

Correct Answer: A 

Question #337

Topic 1

A media firm uses an application to monitor user clicks on its websites and do analytics in order to deliver near-real-time suggestions. The program is implemented as a fleet of Amazon EC2 instances that collect data from websites and transfer it to an Amazon RDS database instance. Another fleet of Amazon EC2 instances hosts the piece of the program that is constantly monitoring the database for changes and performing SQL queries to generate suggestions. Management has ordered a rethink of the infrastructure in order to decouple it. The solution must guarantee that data analysts write SQL only for the purpose of data analysis. There is no possibility of data loss during the deployment.

What recommendations should a solutions architect make?

- A. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
- B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
- C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
- D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

Correct Answer: B 

Question #338

Topic 1

A business developed an application that enables users to check in at locations, score them, and provide opinions about their experiences. The application is a success, with a monthly user base that is rapidly growing.

The chief technology officer is concerned that the database that powers the present infrastructure will be unable to manage the additional demand the following month, since the single Amazon RDS for MySQL instance has generated alerts linked to resource depletion due to read requests.

What can a solutions architect propose to minimize code modifications required to avoid service interruptions at the database layer?

- A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.
- B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.
- C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.
- D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

Correct Answer: A 

Question #339

Topic 1

A healthcare organization maintains extremely confidential patient records. Compliance necessitates the storage of several copies in distinct places. Each record must be retained for a period of seven years. The corporation has a service level agreement (SLA) with government agencies that requires documents to be provided instantly for the first 30 days and then within four hours of a request after that.

What recommendations should a solutions architect make?

- A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.
- B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.
- C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.
- D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

Correct Answer: A 

Question #340

Topic 1

On-premises, a business manages health records. The firm must retain these documents in perpetuity, disable any alterations made to them after they are saved, and audit access at all levels granularly. The chief technology officer (CTO) is worried because millions of data are currently unused by any application and the present infrastructure is running out of capacity. The Chief Technology Officer has asked that a solutions architect build a solution for migrating old data and supporting future records.

Which solutions architect services may be recommended to suit these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Correct Answer: A 

Question #341

Topic 1

A business hosts their application on AWS. The application is hosted on Amazon EC2 instances behind an Elastic Load Balancer and an Amazon DynamoDB database. The organization needs to guarantee that the application may be moved to another AWS Region with the least amount of downtime possible.

What should a solutions architect do to ensure that these criteria are met with the MINIMUM possible downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be executed when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be executed when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Correct Answer: D 

Question #342

Topic 1

A solutions architect is developing a new API that will accept requests from customers using Amazon API Gateway. Request traffic varies significantly; many hours may pass without getting a single request. Asynchronous data processing will occur, but should be finished within a few seconds of a request being made.

Which compute service should the solutions architect instruct the API to call in order to meet the requirements efficiently?

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

Correct Answer: B 

Question #343

Topic 1

A business wishes to migrate a multi-tiered application from its on-premises environment to the AWS Cloud in order to boost the application's performance. The program is divided into levels that connect with one another using RESTful services. When a tier gets overloaded, transactions are dropped. A solutions architect is responsible for developing a solution that addresses these concerns and modernizes the application.

Which solution satisfies these parameters and is the MOST OPTIMAL in terms of operational efficiency?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Correct Answer: D 

Question #344

Topic 1

A business runs an application on an Amazon EC2 instance with a maximum storage requirement of 200 GB. The application is utilized rarely, with mornings and evenings being the busiest times. Disk I/O varies but reaches a maximum of 3,000 IOPS. The company's chief financial officer is worried about expenses and has requested a recommendation from a solutions architect for the most cost-effective storage choice that does not compromise performance.

Which solution should the architect of solutions recommend?

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

Correct Answer: B 

Question #345

Topic 1

A business wishes to share forensic accounting data with an external auditor that is kept in an Amazon RDS DB instance. The auditor has its own Amazon Web Services (AWS) account and demands a copy of the database.

How should the organization share the database with the auditor in a secure manner?

- A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.
- B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.
- C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.
- D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

Correct Answer: A 

Question #346

Topic 1

A business wants to duplicate its data to AWS in order to be able to recover in the case of a catastrophe. A system administrator nowadays has programs that transfer data to an NFS share.

Individual backup files must be retrieved quickly by program administrators in order to address processing issues.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.
- B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.
- C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.
- D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

Correct Answer: D 

Question #347

Topic 1

A business has an ecommerce application that uses an on-premises SQL database to store data. The organization has chosen to move this database to Amazon Web Services (AWS).

However, as part of the migration, the organization wishes to achieve response times of less than a millisecond for frequent read requests.

A solutions architect understands that performance is critical and that a tiny amount of stale data returned during database reads is acceptable.

What recommendations should the solutions architect make?

- A. Build Amazon RDS read replicas.
- B. Build the database as a larger instance type.
- C. Build a database cache using Amazon ElastiCache.
- D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

Correct Answer: A 

Reference:

<https://aws.amazon.com/redis/>

Question #348

Topic 1

A business keeps sensitive user data in an Amazon S3 bucket. The organization wishes to safeguard access to this bucket from the application layer, which is comprised of Amazon EC2 instances operating inside a VPC.

Which actions should a solutions architect use in conjunction to achieve this? (Select two.)

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- B. Create a bucket policy to make the objects in the S3 bucket public.
- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Correct Answer: AC 

Question #349

Topic 1

A business develops a mobile application that enables clients to submit images to a website. The application requires a secure login process that includes multi-factor authentication (MFA). The firm want to minimize the time required to construct and maintain the solution.

Which solution, according to a solutions architect, should be recommended to satisfy these requirements?

- A. Use Amazon Cognito Identity with SMS-based MFA.
- B. Edit IAM policies to require MFA for all users.
- C. Federate IAM against the corporate Active Directory that requires MFA.
- D. Use Amazon API Gateway and require server-side encryption (SSE) for photos.

Correct Answer: A 

Reference:

<https://aws.amazon.com/cognito/>

Question #350

Topic 1

For many years, an application needs a development environment (DEV) and a production environment (PROD). DEV instances will be available for 10 hours per day during regular business hours, whereas PROD instances will be available 24 hours per day. A solutions architect must decide on a strategy for purchasing compute instances in order to reduce expenses.

Which of the following is the MOST cost-effective solution?

- A. DEV with Spot Instances and PROD with On-Demand Instances
- B. DEV with On-Demand Instances and PROD with Spot Instances
- C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances
- D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

Correct Answer: C 

Question #351

Topic 1

An ecommerce website is hosted on Amazon EC2 instances that are managed by an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance difficulties as a result of a significant volume of requests from unauthorized external systems using dynamic IP addresses. The security team is concerned about the possibility of DDoS assaults on the website. The firm must prohibit unauthorized inbound requests in a manner that has the fewest possible adverse effects on legal users.

What recommendations should a solutions architect make?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Correct Answer: B 

Reference:

<https://aws.amazon.com/blogs/aws/protect-web-sites-services-using-rate-based-rules-for-aws-waf/>

Question #352

Permissions are required for a group to list and remove things from an Amazon S3 bucket. To provide access to the bucket, an administrator developed the following IAM policy and applied it to the group. The group does not have the ability to remove items from the bucket. The organization adheres to the principle of least privilege when it comes to access.



Which sentence in the policy should a solutions architect include to rectify bucket access?

A.

```
"Action": [
    "s3:*Object"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

praw709528

B.

```
"Action": [
    "s3:*
```

praw709528

]

```
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

C.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"
```

praw709528

D.

```
"Action": [
    "s3:DeleteObject"
],
"Resource": [
    "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"
```

praw709528

Correct Answer: A

Question #353

Topic 1

A business is considering moving its virtual server-based workloads to AWS. The corporation utilizes load balancers on the internet that are backed up by application servers. Patches are applied to the application servers using an internet-hosted repository.

Which services should a solution architect propose for public subnet hosting? (Select two.)

- A. NAT gateway
- B. Amazon RDS DB instances
- C. Application Load Balancers
- D. Amazon EC2 application servers
- E. Amazon Elastic File System (Amazon EFS) volumes

Correct Answer: AC 

Question #354

Topic 1

A business uses Amazon ECS to execute an application. The program resizes an original picture and then uses the Amazon S3 API to store the scaled photos in Amazon S3.

How can a solutions architect guarantee that an application is granted access to Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B 

Question #355

Topic 1

A MySQL database is used by a company's order fulfillment service. The database must be able to handle a high volume of concurrent requests and transactions. The developers are repairing and adjusting the database. This results in delays in the introduction of new product features. The organization wishes to use cloud-based services in order to assist it in addressing this new difficulty. The solution must enable developers to move the database with little or no modifications to the code and must maximize performance.

Which solution architect service should be used to achieve these requirements?

- A. Amazon Aurora
- B. Amazon DynamoDB
- C. Amazon ElastiCache
- D. MySQL on Amazon EC2

Correct Answer: A 

Question #356

Topic 1

An application makes a request to a vendor-hosted service. The seller charges on a per-call basis. The finance department need information on the number of calls made to the service in order to verify the billing bills.

How can a solutions architect develop a system that can reliably record the number of calls without needing application changes?

- A. Call the service through an internet gateway.
- B. Decouple the application from the service with an Amazon Simple Queue Service (Amazon SQS) queue.
- C. Publish a custom Amazon CloudWatch metric that counts calls to the service.
- D. Call the service through a VPC peering connection.

Correct Answer: C 

There are 2 main types of monitoring you can do on AWS EC2 Instances as follows:

Basic Monitoring for Amazon EC2 instances: Seven pre-selected metrics at five-minute frequency and three status check metrics at one-minute frequency, for no additional charge.

Detailed Monitoring for Amazon EC2 instances: All metrics available to Basic Monitoring at one-minute frequency, for an additional charge.

Instances with Detailed

Monitoring enabled allows data aggregation by Amazon EC2 AMI ID and instance type.

Reference:

<https://datanextsolutions.com/blog/how-to-collect-custom-metrics-from-aws-ec2-instances/>

Question #357

Topic 1

A firm uses AWS to power a popular gaming platform. The program is sensitive to latency since it might degrade the user experience and give certain players an unfair edge. The application is available across all AWS Regions. It is hosted on Amazon EC2 instances that are configured as members of Auto Scaling groups behind Application Load Balancers (ALBs). A solutions architect must include a system for monitoring the application's health and redirecting traffic to healthy endpoints.

Which solution satisfies these criteria?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in- memory cache for DynamoDB hosting the application data.

Correct Answer: D 

Question #358

Topic 1

A business hosts an application on Amazon EC2 instances in two VPCs spread across several AWS Regions. The instances interact with one another over the internet. The security team want to guarantee that no communication occurs over the internet between the instances.

What actions should a solutions architect take to achieve this?

- A. Create a NAT gateway and update the route table of the EC2 instances' subnet.
- B. Create a VPC endpoint and update the route table of the EC2 instances' subnet.
- C. Create a VPN connection and update the route table of the EC2 instances' subnet.
- D. Create a VPC peering connection and update the route table of the EC2 instances' subnet.

Correct Answer: D 

Question #359

Topic 1

A business is operating a publicly available serverless application on AWS Lambda and Amazon API Gateway. Recently, the application's traffic increased significantly as a result of bogus requests from botnets.

Which actions should a solutions architect take to prevent unauthorized users from submitting requests? (Select two.)

- A. Create a usage plan with an API key that is shared with genuine users only.
- B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
- C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
- D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
- E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Correct Answer: AE 

Reference:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiR_oHhu5DyAhVvA2MBHWEbDhgQFjAGegQIihAD&url=https%3A%2F%2Faws.amazon.com%2Fblogs%2Fmedia%2Ftag%2Famazon-api-gateway%2Ffeed%2F&usg=A0vVaw2OaNncetRRtgvJ-d60ePyu

Question #360

Topic 1

A corporation has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-1 Region through an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-1 Region. A solutions architect is creating a disaster recovery plan that will provide the database in the us-west-2 Region in the event that the database becomes inaccessible in the us-east-1 Region. The architecture must guarantee that the database is supplied within a maximum of two hours in the us-west-2 Region, with a maximum data loss window of three hours.

How are these stipulations to be met?

- A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.
- B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.
- C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.
- D. Create a multimaster read/write instances across multiple AWS Regions. Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

Correct Answer: B 

Question #361

Topic 1

A business operates a media shop using several Amazon EC2 instances dispersed across various Availability Zones under a single VPC. The organization need a high-performance solution for data sharing across all EC2 instances, but wishes to retain data inside the VPC.

What recommendations should a solutions architect make?

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

Correct Answer: D 

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/wt1-test.html>

Question #362

Topic 1

In an Amazon S3 bucket, a business is storing 60 TB of production-level data. A solution architect is required to bring the data on-premises in order to comply with quarterly audit requirements. This data export must be encrypted in transit. The corporation uses a low-bandwidth network connection between AWS and its on-premises data center.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.
- B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.
- C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.
- D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

Correct Answer: B 

Question #363

Topic 1

A business is worried that the two NAT instances now in operation would be unable to handle the traffic required for the business's application. A solutions architect wishes to develop a highly available, fault-tolerant, and self-scaling system.

What recommendations should the solutions architect make?

- A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.
- B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.
- C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.
- D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

Correct Answer: C 

Question #364

Topic 1

A business maintains a multi-tiered web application for the purpose of hosting news information. The application is deployed on Amazon EC2 instances that are routed via an Application Load Balancer. The instances are distributed across various Availability Zones through an Amazon EC2 Auto Scaling group and use an Amazon Aurora database. A solution architect must strengthen the application's resistance to frequent spikes in request rates.

Which architecture should be implemented by the solutions architect? (Select two.)

- A. Add AWS Shield.
- B. Add Aurora Replica.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Correct Answer: DE 

AWS Global Accelerator -

Acceleration for latency-sensitive applications

Many applications, especially in areas such as gaming, media, mobile apps, and financials, require very low latency for a great user experience.

To improve the user experience, Global Accelerator directs user traffic to the application endpoint that is nearest to the client, which reduces internet latency and jitter. Global

Accelerator routes traffic to the closest edge location by using Anycast, and then routes it to the closest regional endpoint over the AWS global network. Global

Accelerator quickly reacts to changes in network performance to improve your users' application performance.

Amazon CloudFront -

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

Question #365

Topic 1

A firm is developing a web application on AWS utilizing containers. At any one moment, the organization needs three instances of the web application to be running. The application must be highly available and scalable in order to keep up with demand increases.

Which solution satisfies these criteria?

- A. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
- B. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.
- C. Use the AWS Fargate launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has three container instances in three different Availability Zones. Create a task definition for the web application. Create an ECS service that has a desired count of three tasks.
- D. Use the Amazon EC2 launch type to create an Amazon Elastic Container Service (Amazon ECS) cluster that has one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance. Place one task on the remaining container instance.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-placement.html> <https://aws.amazon.com/blogs/containers/amazon-ecs-availability-best-practices/>

Question #366

Topic 1

A business demands the retention of all versions of items in its Amazon S3 bucket. During the first 30 days, current object versions will be often visited; afterwards, they will be seldom accessed and must be retrievable within 5 minutes. Previous object versions must be retained indefinitely, will be viewed seldom, and may be recovered within a week. All storage options must be very accessible and durable.

What should a solutions architect propose as the MOST cost-effective method of meeting these requirements?

- A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.
- B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.
- D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

Correct Answer: B 

Question #367

Topic 1

A solutions architect is converting a monolithic online application for a client into a multi-tier application. The business wishes to abstain from controlling its own infrastructure. The web application's minimal requirements include high availability, scalability, and regionally low latency during peak hours. Additionally, the solution should save and retrieve data via the application's API with millisecond latency.

Which solution satisfies these criteria?

- A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.
- B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.
- C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.
- D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

Correct Answer: A 

Question #368

Topic 1

A business must reassess its requirements for the Amazon EC2 instances it has supplied in an Auto Scaling group. At the moment, the Auto Scaling group is set to run no less than two instances and no more than four instances across two Availability Zones. A solutions architect evaluated Amazon CloudWatch analytics and discovered that CPU usage for all EC2 instances is consistently low.

What should the solutions architect propose to improve usage while maintaining fault tolerance in the application?

- A. Remove some EC2 instances to increase the utilization of remaining instances.
- B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.
- C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.
- D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

Correct Answer: D 

As the Launch Configuration can't be modified once created, the only way to update the Launch Configuration for an Auto Scaling group is to create a new one and associate it with the Auto Scaling group

Question #369

Topic 1

A firm is installing an application in three AWS Regions utilizing an Application Load Balancer. To distribute traffic across these Regions, Amazon Route 53 will be utilized.

Which Route 53 configuration should a solutions architect employ to get the highest possible performance?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy.
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

Correct Answer: A 

Question #370

Topic 1

Within 30 days, a corporation must move 20 TB of data from a data center to the AWS Cloud. The network capacity of the organization is restricted to 15 Mbps and cannot exceed 70% use.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

Correct Answer: A 

Question #371

Topic 1

An organization hosts an application on Amazon EC2 instances in a private subnet of a VPC. The EC2 instances are configured in an Auto Scaling group and are connected to an Elastic Load Balancer through an Elastic Load Balancer (ELB). For outbound internet connectivity, the EC2 instances make use of a NAT gateway. EC2 instances, on the other hand, are unable to access to the public internet in order to get software updates.

What might be the underlying reasons of this problem? (Select two.)

- A. The ELB is not configured with a proper health check.
- B. The route tables in the VPC are configured incorrectly.
- C. The EC2 instances are not associated with an Elastic IP address.
- D. The security group attached to the NAT gateway is configured incorrectly.
- E. The outbound rules on the security group attached to the EC2 instances are configured incorrectly.

Correct Answer: BD 

Reference:

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html> <https://forums.aws.amazon.com/thread.jspa?threadID=226927>

Question #372

Topic 1

A corporation wishes to impose stringent security controls on access to AWS Cloud resources as it migrates production workloads from its data centers to the cloud.

The company's management desires that all users obtain rights according with their employment titles and responsibilities.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Create an AWS Single Sign-On deployment. Connect to the on-premises Active Directory to centrally manage users and permissions across the company.
- B. Create an IAM role for each job function. Require each employee to call the sts:AssumeRole action in the AWS Management Console to perform their job role.
- C. Create individual IAM user accounts for each employee. Create an IAM policy for each job function, and attach the policy to all IAM users based on their job role.
- D. Create individual IAM user accounts for each employee. Create IAM policies for each job function. Create IAM groups, and attach associated policies to each group. Assign the IAM users to a group based on their job role.

Correct Answer: A 

Reference:

<https://d1.awsstatic.com/whitepapers/adds-on-aws.pdf>

Question #373

Topic 1

A business need guaranteed Amazon EC2 capacity in three specified Availability Zones inside a certain AWS Region for a one-week-long event.

What should the organization do to ensure EC2 capacity is maintained?

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

Correct Answer: D 

Question #374

Topic 1

A provider of online education is transitioning to the AWS Cloud. The company's student records are stored in a PostgreSQL database. The organization need a solution that ensures its data is always available and accessible across several AWS Regions.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C 

Question #375

Topic 1

A solutions architect is improving an on-premises data center's old document management program running on Microsoft Windows Server. The program makes extensive use of a network file sharing to store a huge number of files. The chief information officer wants to lower the footprint of on-premises data centers and storage expenses by migrating on-premises storage to AWS.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Set up an AWS Storage Gateway file gateway.
- B. Set up Amazon Elastic File System (Amazon EFS)
- C. Set up AWS Storage Gateway as a volume gateway
- D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: A 

Question #376

Topic 1

A business keeps symmetric encryption keys in a hardware security module at the moment (HSM). A solutions architect is responsible for designing a solution for key management migration to AWS. Key rotation should be supported, as should the usage of customer-supplied keys.

Where should critical material be housed to ensure compliance with these requirements?

- A. Amazon S3
- B. AWS Secrets Manager
- C. AWS Systems Manager Parameter store
- D. AWS Key Management Service (AWS KMS)

Correct Answer: D 

Question #377

Topic 1

A business has implemented an API in a Virtual Private Cloud (VPC) behind an internet-facing Application Load Balancer (ALB). In a second account, an application that uses the API as a client is installed in private subnets behind a NAT gateway. When the number of requests to the client application increases, the NAT gateway expenses exceed expectations. The ALB has been set to be internal by a solutions architect.

Which architectural improvements will result in the lowest NAT gateway costs? (Select two.)

- A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.
- B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
- C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.
- D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.
- E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

Correct Answer: DE 

Question #378

Topic 1

Recently, a corporation built Linux-based application instances on Amazon EC2 in a private subnet and a Linux-based bastion host on an Amazon EC2 instance in a VPC's public subnet. A solutions architect must establish connections from the on-premises network to the bastion host and application servers through the company's internet connection. The solutions architect must ensure that all EC2 instances' security groups permit this access.

Which measures should the solutions architect do in combination to satisfy these requirements? (Select two.)

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Correct Answer: AC 

Question #379

Topic 1

On AWS, a business want to develop an online marketplace application as a collection of loosely linked microservices. When a client places a new order, two microservices should process the event concurrently in this application. A confirmation email will be sent via the Email microservice, and the OrderProcessing microservice will initiate the order delivery procedure. When a client cancels an order, the OrderCancellation and Email microservices should process the cancellation concurrently.

A solutions architect want to build the communications between microservices using Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS).

What approach should the solutions architect use while designing the solution?

- A. Create a single SQS queue and publish order events to it. The Email OrderProcessing and OrderCancellation microservices can then consume messages of the queue.
- B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email OrderProcessing and OrderCancellation microservices to its own topic.
- C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email OrderProcessing and OrderCancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.
- D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and OrderCancellation microservices.

Correct Answer: D 

Question #380

Topic 1

The application of a business is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are distributed across several Availability Zones through an Amazon EC2 Auto Scaling group. At midnight on the first day of each month, the application becomes much slower when the month-end financial computation batch performs. This causes the CPU usage of the EC2 instances to spike to 100% quickly, causing the application to fail.

What should a solutions architect propose to guarantee that the application can manage the volume without experiencing downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C 

Scheduled Scaling for Amazon EC2 Auto Scaling

Scheduled scaling allows you to set your own scaling schedule. For example, let's say that every week the traffic to your web application starts to increase on

Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Question #381

Topic 1

An application enables users in the corporate headquarters of a business to view product data. The product data is saved in a MySQL database instance hosted by Amazon RDS. The operations team has found a performance delay in the application and want to split read and write traffic. A solutions architect must work fast to optimize an application's performance.

What recommendations should the solutions architect make?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D 

Question #382

Topic 1

A business is developing a website that will read from and write to an Amazon DynamoDB database. The website's traffic is predictable in that it peaks during business hours on weekdays and falls overnight and on weekends. A solutions architect must create a solution that is both cost efficient and capable of handling the demand.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Enable DynamoDB Accelerator (DAX) to cache the data.
- B. Enable Multi-AZ replication for the DynamoDB database.
- C. Enable DynamoDB auto scaling when creating the tables.
- D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

Correct Answer: C 

Question #383

Topic 1

A business maintains a static website through its on-premises data center. Although the firm has many servers that manage all of its traffic, services are sometimes disrupted and the website goes inaccessible on busy days. The corporation wants to have a worldwide footprint and intends to treble its online traffic.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.
- B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.
- C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.
- D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

Correct Answer: D 

Question #384

Topic 1

A business hosts apps on Amazon EC2 instances equipped with IPv6 addresses. Through the internet, the apps must begin communications with other external applications. However, according to the company's security policy, no external service is permitted to start a connection to the EC2 instances.

What should a solutions architect suggest as a remedy to this problem?

- A. Create a NAT gateway and make it the destination of the subnet's route table.
- B. Create an internet gateway and make it the destination of the subnet's route table.
- C. Create a virtual private gateway and make it the destination of the subnet's route table.
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table.

Correct Answer: D 

Question #385

Topic 1

A business has a web application that receives occasional use. Each month, there is a spike in use at the beginning, a minor spike at the start of each week, and an unexpected spike throughout the week. The program is made up of a web server and a MySQL database server that are both located inside the data center. The firm want to migrate the application to the AWS Cloud and needs to choose an affordable database platform that does not need database adjustments.

Which solution will satisfy these criteria?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: B 

Question #386

Topic 1

A business is developing an application that will allow customers to upload tiny files to Amazon S3. After a user uploads a file, it undergoes one-time basic processing to change the data and store it in JSON format for further analysis.

Each file must be handled immediately upon upload. Demand will fluctuate. On some days, people will upload an unusually large amount of files. On other days, people will upload a small number of files or none at all.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.
- B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in Amazon Aurora DB cluster.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-ug.pdf>

Question #387

Topic 1

A business has built a microservices application. It processes user queries using a client-facing API integrated with Amazon API Gateway and several internal services deployed on Amazon EC2 instances. Although the API is built to handle unforeseen traffic spikes, internal services may become overloaded and unavailable for a brief period during surges. A solutions architect must provide a more dependable solution that minimizes mistakes when internal services become unavailable or unresponsive.

Which solution satisfies these criteria?

- A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.
- B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.
- C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.
- D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

Correct Answer: D 

Question #388

Topic 1

A business wishes to transfer an on-premises high performance computing (HPC) application and data to the AWS Cloud. On-premises storage is tiered, with hot high-performance parallel storage supporting the program during periodic runs and more cost-effective cold storage storing data while the application is not actively operating.

Which solution combination should a solutions architect propose to meet the application's storage requirements? (Select two.)

- A. Amazon S3 for cold data storage
- B. Amazon Elastic File System (Amazon EFS) for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD 

Question #389

Topic 1

A company's security policy mandates that all AWS API activity in its AWS accounts be tracked and audited on a regular basis. The firm must activate AWS CloudTrail on all existing and future AWS accounts that use AWS Organizations.

Which of the following solutions is the MOST SECURE?

- A. At the organization's root, define and attach a service control policy (SCP) that permits enabling CloudTrail only.
- B. Create IAM groups in the organization's management account as needed. Define and attach an IAM policy to the groups that prevents users from disabling CloudTrail.
- C. Organize accounts into organizational units (OUs). At the organization's root, define and attach a service control policy (SCP) that prevents users from disabling CloudTrail.
- D. Add all existing accounts under the organization's root. Define and attach a service control policy (SCP) to every account that prevents users from disabling CloudTrail.

Correct Answer: C 

Question #390

Topic 1

A solutions architect is tasked with the responsibility of developing a mission-critical online application. It will be comprised of Amazon EC2 instances connected to a relational database through an Application Load Balancer. The database should have a high degree of availability and should be fault tolerant.

Which database implementations will be able to fulfill these criteria? (Select two.)

- A. Amazon Redshift
- B. Amazon DynamoDB
- C. Amazon RDS for MySQL
- D. MySQL-compatible Amazon Aurora Multi-AZ
- E. Amazon RDS for SQL Server Standard Edition Multi-AZ

Correct Answer: DE 

Question #391

Topic 1

A business is developing a web application that will interface with a content management system. The content management system is hosted on Amazon EC2 instances, which are routed via an Application Load Balancer (ALB). The EC2 instances are distributed across several Availability Zones in an Auto Scaling group. The content management system's users are continually adding and modifying files, blogs, and other website assets.

A solutions architect must design a solution that enables all EC2 instances to exchange current website content with the least amount of lag time feasible.

Which solution satisfies these criteria?

- A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently. Configure the ALB to make changes to the website assets only in the newest EC2 instance.
- B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system. Configure each EC2 instance to mount the EFS file system locally. Configure the website hosting application to reference the website assets that are stored in the EFS file system.
- C. Copy the website assets to an Amazon S3 bucket. Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume. Run the S3 sync command once each hour to keep files up to date.
- D. Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets. Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched. Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Question #392

Topic 1

A single AWS account allows a business to host its internet-facing containerized web application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.

The EKS cluster is located inside a VPC's private subnet. The EKS cluster is accessed by system administrators through a bastion server on a public network.

The company's new security policy prohibits the usage of bastion hosts. Additionally, the organization must prohibit internet access to the EKS cluster.

Which option best fits these criteria in terms of cost-effectiveness?

- A. Set up an AWS Direct Connect connection.
- B. Create a transit gateway.
- C. Establish a VPN connection.
- D. Use AWS Storage Gateway.

Correct Answer: B 

Question #393

Topic 1

A business has a highly dynamic batch processing operation that requires the utilization of a large number of Amazon EC2 instances to finish. The work is stateless in nature, meaning it may be started and stopped at any moment without causing any damage, and normally takes up to 60 minutes to finish. The organization has engaged a solutions architect to develop a scalable and cost-effective solution that satisfies the job's needs.

What recommendations should the solutions architect make?

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

Correct Answer: A 

Question #394

Topic 1

A business has multiple web servers that regularly need access to a shared Amazon RDS MySQL Multi-AZ database instance. The organization requires a safe means for web servers to connect to the database while also adhering to a security requirement that user credentials be rotated on a regular basis.

Which solution satisfies these criteria?

- A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
- B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
- C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
- D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

Question #395

Topic 1

A business is transferring a huge, mission-critical database to Amazon Web Services (AWS). A solutions architect has chosen to utilize an Amazon RDS for MySQL Multi-AZ DB instance with storage capacity of 80,000 Provisioned IOPS. The data transfer is being carried out by the solutions architect utilizing AWS Database Migration Service (AWS DMS). The relocation process is taking longer than anticipated, and the corporation want to expedite it. The network staff at the organization has ruled out bandwidth as a constraint.

How should the solutions architect proceed to expedite the migration? (Select two.)

- A. Disable Multi-AZ on the target DB instance.
- B. Create a new DMS instance that has a larger instance size.
- C. Turn off logging on the target DB instance until the initial load is complete.
- D. Restart the DMS task on a new DMS instance with transfer acceleration enabled.
- E. Change the storage type on the target DB instance to Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2).

Correct Answer: CD 

Question #396

Topic 1

A corporation is considering migrating a mission-critical dataset to Amazon S3. The present solution architecture stores the dataset in a single S3 bucket in the us-east-1 Region with versioning enabled. According to the company's disaster recovery strategy, all data is replicated across various AWS Regions.

How should the S3 solution be designed by a solutions architect?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Correct Answer: C 

Reference:

<https://medium.com/@KerrySheldon/s3-exercise-2-4-adding-objects-to-an-s3-bucket-with-cross-region-replication-a78b332b7697>

Question #397

Topic 1

An ecommerce company's solutions architect want to back up application log data to Amazon S3. The solutions architect has no idea how often or which logs will be accessed. The organization wishes to save expenses by using the suitable S3 storage class.

Which S3 storage type should be used to satisfy these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B 

S3 Intelligent-Tiering -

S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers – frequent access and infrequent access – when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the

S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.999999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

Reference:

<https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/>

Question #398

Topic 1

A business operates an application on Amazon EC2 instances contained inside a private subnet within a VPC. The instances have access to data stored in the same AWS Region's Amazon S3 bucket. To access the S3 bucket, the VPC comprises a NAT gateway on a public subnet. The organization wishes to save money by replacing the NAT gateway without sacrificing security or redundancy.

Which solution satisfies these criteria?

- A. Replace the NAT gateway with a NAT instance.
- B. Replace the NAT gateway with an internet gateway.
- C. Replace the NAT gateway with a gateway VPC endpoint.
- D. Replace the NAT gateway with an AWS Direct Connect connection.

Correct Answer: C 

Question #399

Topic 1

The organizers of a worldwide event want to publish daily reports as static HTML pages online. The pages are anticipated to get millions of views from visitors worldwide. The files are stored in a bucket on Amazon S3. A solutions architect has been tasked with the responsibility of designing a solution that is both efficient and effective.

How should the solutions architect go in order to do this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Correct Answer: D 

Using Amazon S3 Origins, MediaPackage Channels, and Custom Origins for Web Distributions

Using Amazon S3 Buckets for Your Origin

When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket.

You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn't change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

Using Amazon S3 Buckets Configured as Website Endpoints for Your Origin

You can set up an Amazon S3 bucket that is configured as a website endpoint as custom origin with CloudFront.

When you configure your CloudFront distribution, for the origin, enter the Amazon S3 static website hosting endpoint for your bucket. This value appears in the

Amazon S3 console, on the Properties tab, in the Static website hosting pane. For example: <http://bucket-name.s3-website-region.amazonaws.com>

For more information about specifying Amazon S3 static website endpoints, see Website endpoints in the Amazon Simple Storage Service Developer Guide.

When you specify the bucket name in this format as your origin, you can use Amazon S3 redirects and Amazon S3 custom error documents. For more information about Amazon S3 features, see the Amazon S3 documentation.

Using an Amazon S3 bucket as your CloudFront origin server doesn't change it in any way. You can still use it as you normally would and you incur regular

Amazon S3 charges.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html>

Question #400

Topic 1

A business uses Amazon S3 to provide files to select customers who do not have AWS credentials. These users must be granted access for a certain period of time.

What steps should a solutions architect take to ensure that these criteria are met securely?

- A. Enable public access on an Amazon S3 bucket.
- B. Generate a presigned URL to share with the users.
- C. Encrypt files using AWS KMS and provide keys to the users.
- D. Create and assign IAM roles that will grant GetObject permissions to the users.

Correct Answer: B 

Question #401

Topic 1

A business wishes to run its web application on Amazon Web Services (AWS) utilizing numerous Amazon EC2 instances spread across various AWS Regions. Due to the fact that the application content will be region-specific, client requests must be directed to the server that hosts the content for that client location.

What actions should a solutions architect take to achieve this?

- A. Configure Amazon Route 53 with a latency routing policy.
- B. Configure Amazon Route 53 with a weighted routing policy.
- C. Configure Amazon Route 53 with a geolocation routing policy.
- D. Configure Amazon Route 53 with a multivalue answer routing policy

Correct Answer: C 

Question #402

Topic 1

An ecommerce firm is developing an application that will handle payments through a third-party payment provider. The payment provider must expressly permit access to the public IP address of the server making the payment request. However, the company's security regulations prohibit the direct connection of any server to the public internet.

Which solution will satisfy these criteria?

- A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.
- B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.
- C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.
- D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

Correct Answer: B 

Question #403

Topic 1

A solutions architect is tasked with the responsibility of designing a low-latency solution for a static single-page application that users access through a custom domain name. Serverless, encrypted in transit, and cost-effective are all requirements for the solution.

Which AWS services and functionalities should the solutions architect utilize in combination? (Select two.)

- A. Amazon S3
- B. Amazon EC2
- C. AWS Fargate
- D. Amazon CloudFront
- E. Elastic Load Balancer

Correct Answer: AD 

Question #404

Topic 1

A solutions architect must create a network that enables many Amazon EC2 instances to share a single data source for mission-critical data that all EC2 instances may access concurrently. The solution must be highly scalable, simple to install, and compliant with the NFS standard.

Which solution satisfies these criteria?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.
- B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the Instances and apply that to the additional instance.
- C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 Instances that need access to the data.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

Correct Answer: A 

Question #405

Topic 1

A business installs an application on Amazon Web Services Lambda functions that are called using the Amazon API Gateway API. Customer data is stored in an Amazon Aurora MySQL database using Lambda functions. When a corporation updates its database, Lambda functions are prevented from establishing database connections until the upgrade is complete. As a consequence, client data is not captured for some events. A solutions architect must provide a solution that securely maintains customer data generated during database updates.

Which solution will satisfy these criteria?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Correct Answer: A 

Question #406**Topic 1**

An ecommerce firm realized that the performance of their Amazon RDS-based web application had degraded. The reduction in performance is being ascribed to an increase in the amount of read-only SQL queries initiated by business analysts. A solutions architect must resolve the issue with the least amount of modification to the current web application.

What recommendations should the solutions architect make?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: C **Question #407****Topic 1**

A solutions architect is refactoring a monolithic application into two microservices: Microservice A and Microservice B.

Microservice A queues messages for consumption by Microservice B in a central Amazon Simple Queue Service (Amazon SQS) queue. When Microservice B is unable to process a message after four attempts, the message must be withdrawn from the queue and archived for later study.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.
- B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead-letter queue after the message has been received four times.
- C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.
- D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

Correct Answer: B **Question #408****Topic 1**

Amazon EC2 is being used by a business to host its big data analytics workloads. Each night, these variable workloads run, and it is vital that they be completed before the start of business the following day. A solutions architect has been assigned with the responsibility of developing the MOST cost-effective solution possible.

Which approach is most likely to do this?

- A. Spot Fleet
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

Correct Answer: A 

Question #409

Topic 1

A business wants to utilize an AWS Region as a backup site for its on-premises infrastructure. The organization now contains ten terabytes of data and the on-premise data center has a one gigabit per second internet connection. A solutions architect must devise a strategy that enables the organization to migrate its existing data to AWS in 72 hours without utilizing an unencrypted connection.

Which option should the architect choose?

- A. Send the initial 10 TB of data to AWS using FTP.
- B. Send the initial 10 TB of data to AWS using AWS Snowball.
- C. Establish a VPN connection between Amazon VPC and the company's data center.
- D. Establish an AWS Direct Connect connection between Amazon VPC and the company's data center.

Correct Answer: C 

Question #410

Topic 1

A team has developed an application that monitors the upload of new items to an Amazon S3 bucket. The uploads cause an AWS Lambda function to send object information to an Amazon DynamoDB table and a PostgreSQL database hosted by Amazon RDS.

Which of the following actions should the team do to achieve high availability?

- A. Enable Cross-Region Replication in the S3 bucket.
- B. Create a Lambda function for each Availability Zone the application is deployed in.
- C. Enable Multi-AZ on the RDS for PostgreSQL database.
- D. Create a DynamoDB stream for the DynamoDB table.

Correct Answer: C 

Question #411

Topic 1

A business collects and analyzes clickstream data from many websites using batch processing. The data is imported into Amazon Redshift on a nightly basis and is then consumed by business analysts. The organization wishes to transition to near-real-time data processing in order to provide timely insights. The solution should handle streaming data efficiently and with low operational overhead.

Which AWS service combination is the MOST cost-effective for this solution? (Select two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon Kinesis Data Streams
- D. Amazon Kinesis Data Firehose
- E. Amazon Kinesis Data Analytics

Correct Answer: BD

Kinesis Data Streams and Kinesis Client Library (KCL) – Data from the data source can be continuously captured and streamed in near real-time using Kinesis

Data Streams. With the Kinesis Client Library (KCL), you can build your own application that can preprocess the streaming data as they arrive and emit the data for generating incremental views and downstream analysis. Kinesis Data Analytics – This service provides the easiest way to process the data that is streaming through Kinesis Data Stream or Kinesis Data Firehose using SQL. This enables customers to gain actionable insight in near real-time from the incremental stream before storing it in Amazon S3.

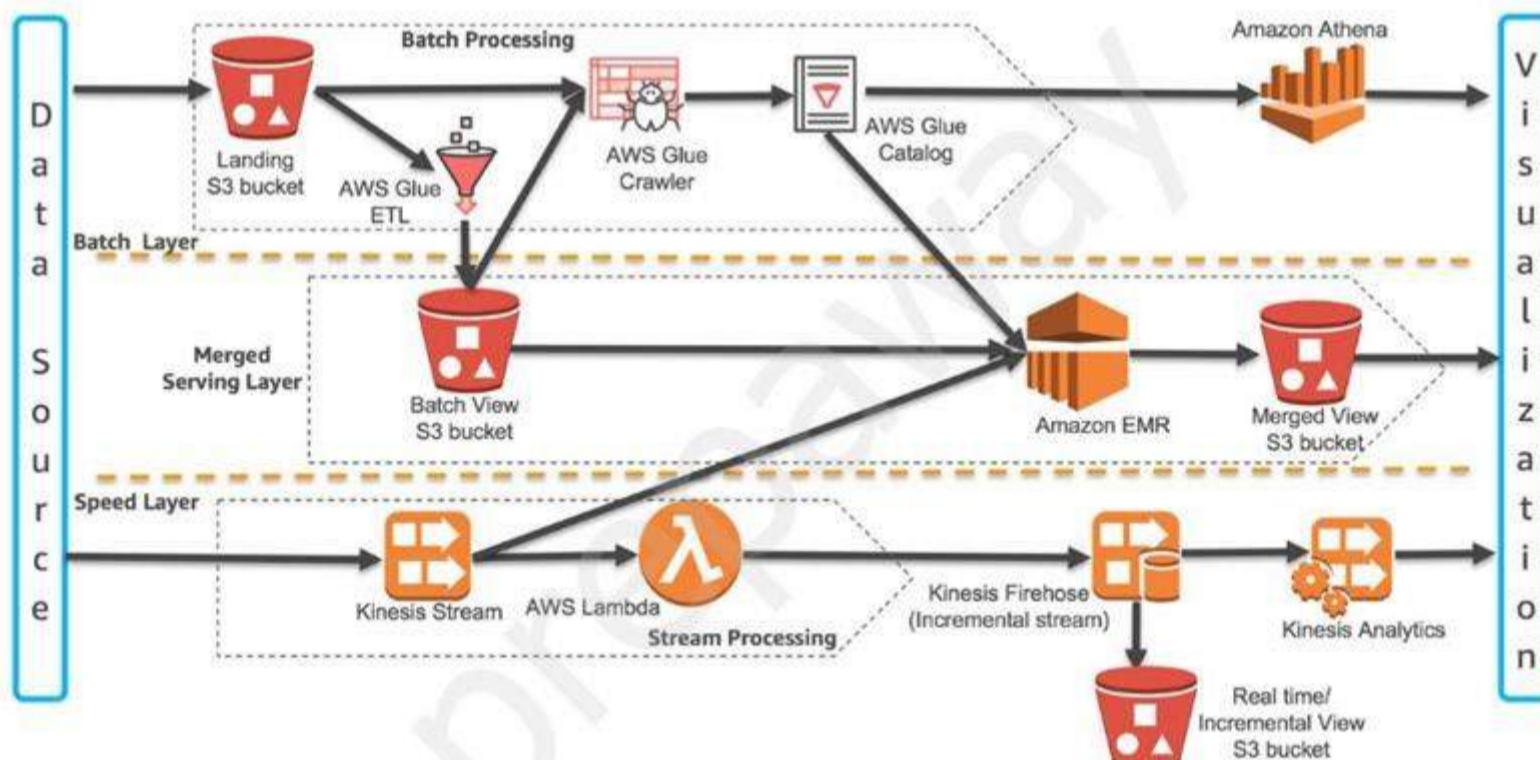


Figure 2: Lambda Architecture Building Blocks on AWS

Reference:

<https://d1.awsstatic.com/whitepapers/lambda-architecure-on-for-batch-aws.pdf>

Question #412

Topic 1

A corporation that provides live video streaming captures and saves real-time data in a disk-optimized database system. The organization is experiencing lower-than-expected throughput and is looking for an in-memory database storage solution that is speedier and delivers high availability via data replication.

Which database should be recommended by a solutions architect?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL.
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Correct Answer: C 

In-memory databases on AWS Amazon ElastiCache for Redis.

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides submillisecond latency to power internet-scale, real-time applications.

Developers can use ElastiCache for Redis as an in-memory nonrelational database. The ElastiCache for Redis cluster configuration supports up to 15 shards and enables customers to run Redis workloads with up to 6.1 TB of in-memory capacity in a single cluster. ElastiCache for Redis also provides the ability to add and remove shards from a running cluster. You can dynamically scaleout and even scale in your Redis cluster workloads to adapt to changes in demand.

Reference:

<https://aws.amazon.com/elasticsearch/redis/faqs/>
<https://aws.amazon.com/nosql/in-memory/>

Question #413

Topic 1

A business is examining a recent transfer of a three-tier application to a virtual private cloud (VPC). The security team detects that the concept of least privilege is not being applied to the entrance and egress rules for Amazon EC2 security groups between application layers.

What actions should a solutions architect take to rectify this situation?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B 

Question #414

Topic 1

A web application operating on an Amazon EC2 instance in VPC-A requires access to files located on another Amazon EC2 instance in VPC-B. Both are distinct AWS accounts. The network administrator must build a solution that enables safe access from VPC-A to an EC2 instance in VPC-B. There should be no single point of failure or issues about bandwidth.

Which solution will satisfy these criteria?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

Correct Answer: D 

Question #415

Topic 1

A business is offering an application that makes use of an Amazon RDS MySQL database. The database must be designed in such a way that it maintains high availability across Availability Zones and AWS Regions with the least amount of downtime possible.

What is the best way for a solutions architect to fulfill this requirement?

- A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.
- B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.
- C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.
- D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

Correct Answer: B 

Question #416

Topic 1

A solutions architect must build a durable solution for the home directories of Windows users. The solution must have fault tolerance, file-level backup and recovery, and access control, all of which must be based on the Active Directory of the business.

Which storage option satisfies these criteria?

- A. Configure Amazon S3 to store the users' home directories. Join Amazon S3 to Active Directory.
- B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.
- C. Configure Amazon Elastic File System (Amazon EFS) for the users' home directories. Configure AWS Single Sign-On with Active Directory.
- D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users' home directories. Configure AWS Single Sign-On with Active Directory.

Correct Answer: B 

Question #417

Topic 1

On Amazon EC2, a business application is hosted and secured object storage is provided by Amazon S3. According to the chief information security officer, no application communication between the two services should pass over the public internet.

Which capabilities should the solution architect use to ensure compliance?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Correct Answer: B 

Question #418

Topic 1

A solutions architect is responsible for designing the architecture of an application that is delivered as a Docker container image by a vendor. The container requires 50 GB of temporary file storage. Serverless infrastructure is required.

Which method satisfies these criteria with the LEAST amount of operational overhead?

- A. Create an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume that has more than 50 GB of space.
- B. Create an AWS Lambda function that uses the Docker container image with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the AWS Fargate launch type. Create a task definition for the container image with an Amazon Elastic File System (Amazon EFS) volume. Create a service with that task definition.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the Amazon EC2 launch type with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space. Create a task definition for the container image. Create a service with that task definition.

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

Question #419

Topic 1

A corporation has an AWS Lambda function that requires read access to an Amazon S3 bucket hosted in the same AWS account as the Lambda function.

Which solution satisfies these criteria the SAFEST way possible?

- A. Apply an S3 bucket policy that grants read access to the S3 bucket.
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Correct Answer: D 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/access-denied-lambda-s3-bucket/>

Question #420

Topic 1

A business operates a website that is protected by numerous Application Load Balancers. The corporation has a variety of distribution rights to its material in several countries. A solutions architect must verify that the proper material is given to users without infringing on distribution rights.

Which configuration should the solution architect use in order to satisfy these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF.
- C. Configure Amazon Route 53 with a geolocation policy.
- D. Configure Amazon Route 53 with a geoproximity routing policy.

Correct Answer: C 

Reference:

[https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
\(geolocation routing\)](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#geolocation-routing)

Question #421

Topic 1

A user requests a list of the IAM roles associated with their Amazon EC2 instance. The user has access to the EC2 instance through the login interface but does not have IAM rights.

.How might a solutions architect go about retrieving this data?

- A. Run the following EC2 command: curl http://169.254.169.254/latest/meta-data/iam/info
- B. Run the following EC2 command: curl http://169.254.169.254/latest/user-data/iam/info
- C. Run the following EC2 command: http://169.254.169.254/latest/dynamic/instance-identity/
- D. Run the following AWS CLI command: aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

Correct Answer: A 

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

Question #422

Topic 1

A solutions architect has established a new AWS account and is responsible for securing root user access to the account.

Which action(s) will do this? (Select two.)

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: AB 

Question #423

Topic 1

A bicycle sharing firm is building a multi-tier architecture to monitor the position of its bicycles during peak hours of operation. The business intends to incorporate these data points into its current analytics platform. A solutions architect must decide on the most suitable multi-tier architectural support choice. The REST API must be able to access the data points.

Which action satisfies these storage and retrieval criteria for location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Correct Answer: D 

Reference:

<https://aws.amazon.com/kinesis/data-analytics/>

Question #424

Topic 1

A business runs a multi-tier web application that stores data on an Amazon Aurora MySQL DB cluster. Amazon EC2 instances are used to host the application tier. The company's information technology security policies require that database credentials be encrypted and cycled every 14 days.

What should a solutions architect do in order to satisfy this demand with the LEAST amount of operational work possible?

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

Correct Answer: B 

Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

Question #425

Topic 1

A business is expanding as demand for its goods increases. When traffic increases, the company's current purchase application is sluggish. The application is a three-layer monolith that employs synchronous transactions and sometimes has bottlenecks at the application tier. A solutions architect must build a solution that satisfies application response time requirements while allowing for surges in traffic flow.

Which solution will satisfy these criteria?

- A. Vertically scale the application instance using a larger Amazon EC2 instance size.
- B. Scale the application's persistence layer horizontally by introducing Oracle RAC on AWS.
- C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.
- D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

Correct Answer: C 

Question #426

Topic 1

A solutions architect is tasked with developing the storage architecture for a new online application that will be used to store and display engineering drawings. All application components will be hosted on AWS.

The application's architecture must use caching in order to decrease the time users spend waiting for engineering drawings to load. Petabytes of data must be able to be stored in the program.

Which storage and caching mix should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Correct Answer: B 

Question #427

Topic 1

A media business is considering migrating its operations to the AWS Cloud. The organization requires at least ten terabytes of storage with the highest feasible I/O performance for video processing, 300 terabytes of very durable storage for media content storage, and 900 terabytes of storage to satisfy standards for archiving material that is no longer in use.

Which services should a solutions architect propose in order to satisfy these requirements?

- A. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon Elastic Block Store (Amazon EBS) for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon Elastic File System (Amazon EFS) for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: A 

Question #428

Topic 1

A business seeks a storage solution that allows its data science team to study data both on-premises and on the Amazon Web Services (AWS) Cloud. The team must be able to conduct statistical studies on-premises and through a fleet of Amazon EC2 instances distributed across several Availability Zones.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.
- B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.
- C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

Correct Answer: C 

Question #429

Topic 1

A business wishes to transfer its MySQL database from its on-premises location to AWS. The organization recently had a database outage, which had a substantial effect on business operations. To prevent this from happening again, the organization need a scalable database solution on AWS that minimizes data loss and replicates each transaction over at least two nodes.

Which solution satisfies these criteria?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B 

Question #430

Topic 1

A business is auditing its AWS Cloud deployment to guarantee that no one may access its data without the proper authorisation. A solutions architect is responsible for identifying all open Amazon S3 buckets and documenting any modifications to their setup.

What is the solution architect's role in achieving this?

- A. Enable AWS Config service with the appropriate rules
- B. Enable AWS Trusted Advisor with the appropriate checks.
- C. Write a script using an AWS SDK to generate a bucket report
- D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

Correct Answer: A 

Question #431

Topic 1

A business owns an asynchronous API that is used to ingest user requests and route them to the appropriate microservice for processing depending on the request type. The firm is deploying the API front end using Amazon API Gateway, as well as an AWS Lambda function that calls Amazon DynamoDB to store user requests before routing them to the processing microservices.

The firm supplied as much DynamoDB capacity as possible within its budget constraints, yet the company continues to have availability difficulties and is losing user requests.

What should a solutions architect do to handle this problem in a way that does not negatively effect current users?

- A. Add throttling on the API Gateway with server-side throttling limits.
- B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
- C. Create a secondary index in DynamoDB for the table with the user requests.
- D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Correct Answer: B 

Question #432

Topic 1

A business has 150 TB of on-premises archival picture data that must be migrated to the AWS Cloud within the next month. The company's present network connection supports uploads of up to 100 Mbps for this purpose only at night.

What is the MOST COST-EFFECTIVE method for moving this data and adhering to the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

Correct Answer: B 

Question #433

Topic 1

On-premises, a business runs a multi-tier web application. The web application is containerized and operates on a distributed network of Linux computers that are linked to a PostgreSQL database that stores user records. The operational costs associated with infrastructure maintenance and capacity planning are impeding the company's expansion. A solutions architect must enhance the infrastructure of the application.

Which activities should the solutions architect take in conjunction to achieve this? (Select two.)

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: CD 

Question #434

Topic 1

A start-up business in the us-east-1 Region has a web application operating on several Amazon EC2 instances behind an Application Load Balancer across different Availability Zones. As the company's user base expands in the us-west-1 Region, it requires a low-latency, high-availability solution.

What actions should a solutions architect take to achieve this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Correct Answer: C 

Register endpoints for endpoint groups: You register one or more regional resources, such as Application Load Balancers, Network Load Balancers, EC2

Instances, or Elastic IP addresses, in each endpoint group. Then you can set weights to choose how much traffic is routed to each endpoint. Endpoints in AWS Global Accelerator

Endpoints in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. A static IP address serves as a single point of contact for clients, and Global Accelerator then distributes incoming traffic across healthy endpoints. Global Accelerator directs traffic to endpoints by using the port (or port range) that you specify for the listener that the endpoint group for the endpoint belongs to.

Each endpoint group can have multiple endpoints. You can add each endpoint to multiple endpoint groups, but the endpoint groups must be associated with different listeners.

Global Accelerator continually monitors the health of all endpoints that are included in an endpoint group. It routes traffic only to the active endpoints that are healthy. If Global Accelerator doesn't have any healthy endpoints to route traffic to, it routes traffic to all endpoints.

Reference:

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints.html> <https://aws.amazon.com/global-accelerator/faqs/>

Question #435

Topic 1

A Solutions Architect is responsible for developing a web application that will be hosted on AWS and will enable customers to pay access to premium, shared content stored in an S3 bucket. After purchase, users will have 14 days to download material before being banned access.

Which of the following would require the LEAST amount of effort to implement?

- A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.
- B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.
- C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.
- D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

Correct Answer: C 

Question #436

Topic 1

A web application that is accessible to the public queries a database that is housed on an Amazon EC2 instance in a private subnet. Numerous queries have numerous database joins, and the application's performance has deteriorated as a result of the growth in complicated queries. The application team will be making performance enhancements.

What recommendations should a solutions architect provide to the application team? (Select two.)

- A. Cache query data in Amazon SQS
- B. Create a read replica to offload queries
- C. Migrate the database to Amazon Athena
- D. Implement Amazon DynamoDB Accelerator to cache data.
- E. Migrate the database to Amazon RDS

Correct Answer: BE 

Question #437

Topic 1

The application of a business is hosted on Amazon EC2 instances in a single Region. In the case of a catastrophe, a solutions architect must guarantee that resources are also available for deployment to a secondary Region.

Which activities should the solutions architect take in conjunction to achieve this? (Select two.)

- A. Detach a volume on an EC2 instance and copy it to Amazon S3.
- B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.
- C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
- D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.
- E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

Correct Answer: BD 

Cross Region EC2 AMI Copy -

We know that you want to build applications that span AWS Regions and we're working to provide you with the services and features needed to do so. We started out by launching the EBS Snapshot Copy feature late last year. This feature gave you the ability to copy a snapshot from Region to Region with just a couple of clicks. In addition, last month we made a significant reduction (26% to 83%) in the cost of transferring data between AWS Regions, making it less expensive to operate in more than one AWS region.

Today we are introducing a new feature: Amazon Machine Image (AMI) Copy. AMI Copy enables you to easily copy your Amazon Machine Images between AWS

Regions. AMI Copy helps enable several key scenarios including:

Simple and Consistent Multi-Region Deployment  You can copy an AMI from one region to another, enabling you to easily launch consistent instances based on the same AMI into different regions.

Scalability  You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location.

Performance  You can increase performance by distributing your application and locating critical components of your application in closer proximity to your users.

You can also take advantage of region-specific features such as instance types or other AWS services.

Even Higher Availability  You can design and deploy applications across AWS regions, to increase availability.

Once the new AMI is in an Available state the copy is complete.

Reference:

<https://aws.amazon.com/blogs/aws/ec2-ami-copy-between-regions/>

Question #438

Topic 1

A firm is developing a media sharing service and has chosen to store it on Amazon S3. When a media file is uploaded, the firm initiates a multi-step process that includes creating thumbnails, identifying objects within the photos, transcoding films into standard formats and resolutions, and extracting and storing information in an Amazon DynamoDB database. Metadata is used to facilitate search and navigation. The volume of traffic varies. The system must be scalable to accommodate surges in traffic without incurring additional costs.

What solutions architect recommendations should be made to accommodate this workload?

- A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

Correct Answer: C 

Question #439

Topic 1

A solutions architect must develop an automated solution to a company's compliance policy that prohibits security groups from including a rule allowing SSH from 0.0.0.0/0. If there is a violation of the policy, the business must be informed. A solution is required immediately.

What actions should the solutions architect take to ensure that these criteria are met with the LEAST amount of operational overhead possible?

- A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.
- B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
- C. Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.
- D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

Correct Answer: B 

Reference:

<https://www.stratoscale.com/blog/compute/aws-security-groups-5-best-practices/>

Question #440

Topic 1

A solutions architect is tasked with the responsibility of building the cloud architecture for a new application that will be deployed on AWS. The program enables users to download and upload files interactively. Files older than two years will get limited access. The architect of the solution must guarantee that the application scales to any number of files while ensuring excellent availability and durability.

Which scalable solutions should be recommended by the solutions architect? (Select two.)

- A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.
- B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)
- C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).
- D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.
- E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

Correct Answer: AC 

Question #441

Topic 1

A business intends to utilize Amazon S3 to store user-uploaded photos. At rest, the photos must be secured in Amazon S3. The business does not want to spend time maintaining and rotating the keys, but does wish to regulate who has access to them.

What tools and techniques should a solutions architect use to do this?

- A. Server-Side Encryption with keys stored in an S3 bucket
- B. Server-Side Encryption with Customer-Provided Keys (SSE-C)
- C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Correct Answer: D 

"Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom."

Server-Side Encryption: Using SSE-KMS

You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSE-S3, SSE-C, or SSE-KMS.

SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see Protecting Data Using Server-Side

Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

SSE-C requires that you manage the encryption key. For more information about SSE-C, see Protecting Data Using Server-Side Encryption with Customer-

Provided Encryption Keys (SSE-C).

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS.

The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

You can request encryption and select a CMK by using the Amazon S3 console or API. In the console, check the appropriate box to perform encryption and select your CMK from the list. For the Amazon S3 API, specify encryption and choose your CMK by setting the appropriate headers in a GET or PUT request.

Reference:

<https://aws.amazon.com/kms/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse>

Question #442

Topic 1

Multiple production apps are hosted by a business. One of the apps utilizes Amazon EC2, AWS Lambda, Amazon RDS, Amazon Simple Notification Service (Amazon SNS), and Amazon Simple Queue Service (Amazon SQS) resources distributed across various AWS Regions. All business resources are labeled with the tag 'application' and a value unique to each application. A solutions architect's job is to offer the simplest method for recognizing all labeled components.

Which solution satisfies these criteria?

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

Correct Answer: D 

Question #443

Topic 1

A business wants to employ Amazon Web Services' (AWS) high performance computing (HPC) infrastructure for financial risk modeling. Linux is used to execute the company's HPC workloads. Each HPC process is short-lived, operates on hundreds of Amazon EC2 Spot Instances, and creates thousands of output files that are eventually kept in persistent storage for analytics and long-term future usage.

The organization is looking for a cloud storage solution that enables the transfer of on-premises data to long-term persistent storage, making it accessible to all EC2 instances for processing. Additionally, the solution should provide a fast file system coupled with persistent storage for reading and writing datasets and output files.

Which AWS service combination satisfies these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A 

Question #444

Topic 1

A solutions architect is responsible for developing the cloud architecture for a business that requires hosting hundreds of machine learning models for its customers. The models need up to 10 GB of data from Amazon S3 to be loaded into memory on launch, but do not require disk access. Although the majority of models are used seldom, customers want them to be highly available, accessible, and with minimal latency.

Which option satisfies the specifications and is the MOST cost-effective?

- A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.
- B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.
- C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.
- D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

Correct Answer: C 

Question #445

Topic 1

A meteorological startup business has developed a bespoke web application with the purpose of selling weather data online to its subscribers. The firm now stores its data in Amazon DynamoDB and want to develop a new service that notifies the managers of four internal teams whenever a new weather event is recorded. The firm does not want for this new service to have an adverse effect on the functioning of the existing application.

What actions should a solutions architect take to ensure that these criteria are met with the LEAST amount of operational overhead possible?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Correct Answer: A 

Question #446

Topic 1

A business uses a VPC peering plan to link all of its VPCs inside a same Region in order to facilitate cross-communication. Recent growth in account creation and VPCs has made it more difficult to sustain the VPC peering strategy, and the business anticipates reaching hundreds of VPCs. Additionally, there are fresh demands for the creation of site-to-site VPNs with some of the VPCs. A solutions architect has been charged with the responsibility of establishing a centrally controlled networking infrastructure for various accounts, virtual private clouds, and VPNs.

Which networking solution satisfies these criteria?

- A. Configure shared VPCs and VPNs and share to each other.
- B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.
- C. Configure an AWS Direct Connect connection between all VPCs and VPNs.
- D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

Correct Answer: D 

Question #447

Two IAM policies have been written by a solutions architect: Policy1 and Policy2. Each policy is associated with an IAM group.

Policy1

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

Policy2

```
{  
    "version": "2012-10-17",  
    "statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ds>Delete*",  
            "Resource": "*"  
        }  
    ]  
}
```

A cloud engineer is added to the IAM group as an IAM user.

Which of the following actions will the cloud engineer be able to carry out?

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

Correct Answer: C 

Question #448**Topic 1**

A solutions architect is responsible for building an architecture that will support the operation of a third-party database server. The database software is memory heavy and is licensed on a CPU-based basis, with the cost increasing in direct proportion to the number of virtual CPU cores in the operating system. The solutions architect must choose an Amazon EC2 instance with adequate RAM to operate the database software, yet with a high number of vCPUs. The solutions architect must guarantee that the virtual CPUs are not underutilized and must keep expenditures to a minimum.

Which solution satisfies these criteria?

- A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.
- B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.
- C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.
- D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

Correct Answer: A **Question #449****Topic 1**

A business owns a mobile game that derives the majority of its information from an Amazon RDS database instance. As the game's popularity grew, the creators observed slowdowns in the game's metadata loading times. According to performance metrics, merely scaling the database will not assist. A solutions architect must consider all available choices, which may include snapshot replication and sub-millisecond response times.

What recommendations should the solutions architect make to resolve these issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

Correct Answer: B **Question #450****Topic 1**

A workload is executing on an Amazon EC2 instance and requires millisecond latency. The program does many little file system reads and writes, yet the file system itself is small.

Which volume type of Amazon Elastic Block Store (Amazon EBS) should a solutions architect connect to an EC2 instance?

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

Correct Answer: B 

Reference:

<https://aws.amazon.com/blogs/database/best-storage-practices-for-running-production-workloads-on-hosted-databases-with-amazon-rds-or-amazon-ec2/>

Question #451

Topic 1

A solutions architect is creating a two-tiered architecture with distinct private subnets for compute and database resources. AWS Lambda functions deployed in compute subnets need database connection.

Which option would provide the MOST SECURE connectivity?

- A. Configure the Lambda function to use Amazon RDS Proxy outside the VPC.
- B. Associate a security group with the Lambda function. Authorize this security group in the database's security group.
- C. Authorize the compute subnet's CIDR ranges in the database's security group.
- D. During the initialization phase, authorize all IP addresses in the database's security group temporarily. Remove the rule after the initialization is complete.

Correct Answer: B 

Question #452

Topic 1

A business has deployed a multi-tier application on many Amazon EC2 instances in an Auto Scaling group. Amazon RDS for Oracle instances serve as the application's data layer, using Oracle-native PL/SQL operations. The application's traffic has been continuously rising. This overloads the EC2 instances and causes the RDS instance to run out of storage. The Auto Scaling group lacks scaling metrics and instead specifies the minimal healthy instance count. According to the corporation, traffic will continue to grow at a constant but unpredictable pace until it reaches a plateau.

What should a solutions architect do to guarantee that the system can grow automatically as traffic increases? (Select two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Correct Answer: AC 

Question #453*Topic 1*

A business just established hybrid cloud access with AWS Direct Connect and is now moving data to Amazon S3. The organization is seeking a fully managed solution that would automate and expedite data replication between on-premises storage systems and Amazon Web Services (AWS) storage services.

Which solution should a solutions architect propose for maintaining the confidentiality of the data?

- A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
- B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
- C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.
- D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

Correct Answer: A **Question #454***Topic 1*

A solutions architect is assisting a developer with the design of a new ecommerce shopping cart application utilizing Amazon Web Capabilities (AWS) services. The developer is unclear about the database schema in use and anticipates changing it as the ecommerce site expands. The solution must be very durable and capable of scaling read and write capacity automatically.

Which database solution satisfies these criteria?

- A. Amazon Aurora PostgreSQL
- B. Amazon DynamoDB with on-demand enabled
- C. Amazon DynamoDB with DynamoDB Streams enabled
- D. Amazon SQS and Amazon Aurora PostgreSQL

Correct Answer: B **Question #455***Topic 1*

A business has an aging application that handles data in two distinct stages. Because the second stage of the process takes longer than the first, the firm opted to redesign the application as two distinct microservices running on Amazon ECS.

What is the best way for a solutions architect to incorporate microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Correct Answer: D 

Question #456**Topic 1**

A business's website is hosted on Amazon S3. Monthly, the website provides petabytes of outbound traffic, accounting for the majority of the company's AWS charges.

What actions should a solutions architect do to save money?

- A. Configure Amazon CloudFront with the existing website as the origin.
- B. Move the website to Amazon EC2 with Amazon Elastic Block Store (Amazon EBS) volumes for storage.
- C. Use AWS Global Accelerator and specify the existing website as the endpoint.
- D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

Correct Answer: A **Question #457****Topic 1**

A business wishes to use a customized distributed program for the purpose of calculating numerous profit and loss situations. To do this, the business must establish a network connection between its Amazon EC2 instances. The connection must have a low latency and a high throughput.

Which solution will satisfy these criteria?

- A. Provision the application to use EC2 Dedicated Hosts of the same instance type.
- B. Configure a placement group for EC2 instances that have the same instance type.
- C. Use multiple AWS elastic network interfaces and link aggregation.
- D. Configure AWS PrivateLink for the EC2 instances.

Correct Answer: B 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/network-throughput-benchmark-linux-ec2/>

Question #458**Topic 1**

A corporation is building a real-time multiplier game that communicates with clients and servers through UDP in an Auto Scaling group. Daytime demand spikes are predicted, and the game server platform must respond appropriately. Developers wish to store gamer scores and other non-relational data in a scalable database system.

Which solution, if any, should a solutions architect suggest?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Correct Answer: B 

Question #459

Topic 1

A standard established by an operations team says that IAM policies should not be implemented directly to users. Certain new team members have failed to adhere to this norm. The operations manager need a simple method for identifying users who have attached policies.

What actions should a solutions architect take to achieve this?

- A. Monitor using AWS CloudTrail.
- B. Create an AWS Config rule to run daily.
- C. Publish IAM user changes to Amazon SNS.
- D. Run AWS Lambda when a user is modified.

Correct Answer: C 

Question #460

Topic 1

On Amazon EC2, a solutions architect is developing a high performance computing (HPC) workload. The EC2 instances must connect regularly with one another, necessitating network performance with low latency and high throughput.

Which EC2 setup satisfies these criteria?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Correct Answer: A 

Placement groups -

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload. Depending on the type of workload.

Cluster  packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Question #461**Topic 1**

A business is transferring its data center and need a safe data transfer of 50 TB to AWS within two weeks. The present data center has a 90 percent used Site-to-Site VPN connection to AWS.

Which Amazon Web Services offering could a solutions architect use to achieve these requirements?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized
- D. AWS Storage Gateway

Correct Answer: C **Question #462****Topic 1**

A business wishes to lower the cost of Amazon S3 storage in its production environment while maintaining the durability and performance of the stored items.

What is the FIRST move that the business should take to accomplish these goals?

- A. Enable Amazon Macie on the business-critical S3 buckets to classify the sensitivity of the objects.
- B. Enable S3 analytics to identify S3 buckets that are candidates for transitioning to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Enable versioning on all business-critical S3 buckets.
- D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

Correct Answer: D **Question #463****Topic 1**

A business hosts its static website in an Amazon S3 bucket, which is where Amazon CloudFront gets its start. The business serves customers in the United States, Canada, and Europe and is looking to cut expenses.

What recommendations should a solutions architect make?

- A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.
- B. Implement CloudFront events with Lambda@Edge to run the website's data processing.
- C. Modify the CloudFront price class to include only the locations of the countries that are served.
- D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

Correct Answer: C 

Question #464

Topic 1

A solution architect is tasked with the responsibility of designing a highly available program that consists of web, application, and database layers. HTTPS content delivery should occur as near to the edge as practicable, with the least amount of time required for delivery.

Which solution satisfies these criteria and is the MOST SECURE?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Amazon EC2 instances in private subnets. Configure a public Application Load Balancer with multiple redundant Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Correct Answer: B 

Question #465

Topic 1

A firm that hosts its web application on Amazon Web Services (AWS) needs to verify that all Amazon EC2 instances, Amazon RDS database instances, and Amazon Redshift clusters are tagged. The organization wishes to reduce the time and effort required to configure and operate this check.

What actions should a solutions architect take to achieve this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Correct Answer: A 

Reference:

<https://d1.awsstatic.com/whitepapers/aws-tagging-best-practices.pdf>

Question #466**Topic 1**

A business depends on an application that requires at least four Amazon EC2 instances for normal traffic and up to twelve EC2 instances for peak loads.

The application is mission-critical to the company and must maintain a high level of availability.

Which solution will satisfy these criteria?

- A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.
- B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.
- C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.
- D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

Correct Answer: C **Question #467****Topic 1**

A new AWS customer creates a Site-to-Site VPN between its on-premises datacenter and AWS. According to the firm's security policy, traffic originating on-premises shall remain inside the private IP space of the company while talking with an Amazon Elastic Container Service (Amazon ECS) cluster containing a sample web application.

Which solution satisfies this criterion?

- A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.
- B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.
- C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.
- D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

Correct Answer: C **Question #468****Topic 1**

A business seeks to construct a scalable key management infrastructure to assist developers in encrypting data inside their apps.

How might a solutions architect alleviate operational burdens?

- A. Use multi-factor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Correct Answer: B 

Reference:

<https://aws.amazon.com/kms/faqs/>

Question #469**Topic 1**

A solutions architect is entrusted with the responsibility of moving 750 TB of data from an on-premises network-attached file system to an Amazon S3 Glacier at a branch office.

The migration must not exceed the 1 Mbps internet connection on-premises.

Which solution will satisfy these criteria?

- A. Create an AWS site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Transfer the files directly by using the AWS CLI.
- B. Order 10 AWS Snowball Edge Storage Optimized devices, and select an S3 Glacier vault as the destination.
- C. Mount the network-attached file system to an S3 bucket, and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.
- D. Order 10 AWS Snowball Edge Storage Optimized devices, and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Correct Answer: *B* **Question #470****Topic 1**

A solutions architect must create a solution that stores a static website using Amazon CloudFront and an Amazon S3 origin. According to the company's security policy, every website traffic must be reviewed by AWS WAF.

How should the solutions architect adhere to these specifications?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Correct Answer: *D* **Question #471****Topic 1**

A solutions architect notices that a nightly batch processing operation is automatically scaled up for an additional hour prior to reaching the targeted Amazon EC2 capacity. Every night, the peak capacity is the same, and batch operations always begin at 1 a.m. The solutions architect must create a cost-effective approach that enables rapid attainment of the targeted EC2 capacity while allowing the Auto Scaling group to scale down once the batch processes are complete.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: *C* 

Question #472

Topic 1

A business recently revised its internal security policies. The organization must now verify that all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted using keys generated and cycled on a periodic basis by internal security professionals. To do this, the organization is searching for a native, software-based AWS solution.

What solution should a solutions architect recommend?

- A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.
- B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.
- C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.
- D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

Correct Answer: A 

Question #473

Topic 1

A business has NFS servers in an on-premises data center that need frequent backups to Amazon S3.

Which option satisfies these criteria and is the MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

Correct Answer: C 

Question #474

Topic 1

A solutions architect is tasked with the responsibility of building a multi-region disaster recovery solution for an application that will enable public API access. To load application code, the application will use Amazon EC2 instances with a userdata script and an Amazon RDS for MySQL database. Three hours is the Recovery Time Objective (RTO), while twenty-four hours is the Recovery Point Objective (RPO).

Which architecture would be the LEAST EXPENSIVE to achieve these requirements?

- A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the userdata script. Deploy separate RDS instances in each Region.
- B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script. Create a read replica of the RDS instance in a backup Region.
- C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the userdata script. Create a MySQL read replica of the RDS instance in a backup Region.
- D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the userdata script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

Correct Answer: D 

Question #475

Topic 1

A business intends to develop a new web application using AWS. The firm anticipates consistent traffic for the most of the year and very high traffic on occasion. The web application must be highly available, fault resistant, and have a low response time.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.
- B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.
- C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.
- D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

Correct Answer: B 

Question #476

Topic 1

A business wants to use a hybrid workload for data processing. The data must be available through an NFS protocol to on-premises applications for local data processing, as well as via the AWS Cloud for further analytics and batch processing.

Which solution will satisfy these criteria?

- A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.
- B. Use an AWS Storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.
- C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.
- D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

Correct Answer: A 

Reference:

<https://aws.amazon.com/storagegateway/file/>

Question #477

Topic 1

A business is operating a two-tier ecommerce website on AWS. The existing architecture makes use of a publish-facing Elastic Load Balancer to route traffic to Amazon EC2 instances located inside a private subnet. Static material is housed on Amazon Web Services instances, while dynamic content is accessed from a MySQL database. The application is currently only available in the United States. Recently, the corporation began selling to consumers in Europe and Australia. A solutions architect must create solutions in such a way that International users benefit from an enhanced browsing experience.

Which option is the MOST CHEAPEST?

- A. Host the entire website on Amazon S3.
- B. Use Amazon CloudFront and Amazon S3 to host static images.
- C. Increase the number of public load balancers and EC2 instances.
- D. Deploy the two-tier website in AWS Regions in Europe and Australia.

Correct Answer: B 

Question #478**Topic 1**

A corporation uses AWS to power its two-tier ecommerce website. The web tier is comprised of a load balancer that routes traffic to Amazon Elastic Compute Cloud machines. The database layer is implemented using an Amazon RDS database instance. The EC2 instances and the RDS database instance should not be made publicly accessible. Internet connectivity is required for the EC2 instances to complete payment processing of orders through a third-party web service. The application must have a high degree of availability.

Which setup alternatives will satisfy these requirements? (Select two.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: AB **Question #479****Topic 1**

A solutions architect must verify that any volumes recovered from unencrypted EBC snapshots are encrypted.

What is the solution architect's role in achieving this?

- A. Enable EBS encryption by default for the AWS Region.
- B. Enable EBS encryption by default for the specific volumes.
- C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.
- D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#volume-account-off>

Question #480

Topic 1

Every 90 days, a security team must enforce the rotation of all IAM users' access keys. If an access key is discovered to be older, it must be disabled and deleted. A solutions architect must design a solution that will detect and remediate keys that are more than 90 days old.

Which method satisfies these criteria with the LEAST amount of operational effort?

- A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.
- C. Create an AWS Config rule to check for the key age. Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key.

Correct Answer: A 

Reference:

<https://aws.amazon.com/blogs/mt/managing-aged-access-keys-through-aws-config-remediations/>

Question #481

Topic 1

A business is developing containerized apps. The firm wishes to shift its on-premises development and operational services to AWS. According to management, production systems should be cloud agnostic and share configuration and administrator tools across all production systems. A solutions architect must provide a managed solution that ensures the alignment of open-source software.

Which solution satisfies these criteria?

- A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.
- B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.
- C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.
- D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

Correct Answer: B 

Question #482

Topic 1

A business runs an application that facilitates the upload of files to an Amazon S3 bucket. After files are uploaded, they are analyzed for metadata extraction, which takes less than 5 seconds. The upload volume and frequency vary between a few files per hour to hundreds of concurrent uploads. The organization has commissioned a solutions architect to create a cost-effective architecture that satisfies these needs.

What recommendations should the solutions architect make?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

Correct Answer: B 

Question #483

Topic 1

A business has a multi-tier application that is hosted on six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone and is protected by an Application Load Balancer (ALB). Without affecting the application, a solutions architect must adapt the infrastructure to make it highly accessible.

Which architecture should the solutions architect use to ensure maximum availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: B 

Expanding Your Scaled and Load-Balanced Application to an Additional Availability Zone.

When one Availability Zone becomes unhealthy or unavailable, Amazon EC2 Auto Scaling launches new instances in an unaffected zone. When the unhealthy

Availability Zone returns to a healthy state, Amazon EC2 Auto Scaling automatically redistributes the application instances evenly across all of the zones for your

Auto Scaling group. Amazon EC2 Auto Scaling does this by attempting to launch new instances in the Availability Zone with the fewest instances. If the attempt fails, however, Amazon EC2 Auto Scaling attempts to launch in other Availability Zones until it succeeds.

You can expand the availability of your scaled and load-balanced application by adding an Availability Zone to your Auto Scaling group and then enabling that zone for your load balancer. After you've enabled the new Availability Zone, the load balancer begins to route traffic equally among all the enabled zones.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

Question #484**Topic 1**

A web application development business has deployed hundreds of Application Load Balancers (ALBs) across several regions. The firm want to build an allow list for all load balancers' IP addresses on its firewall device. A solutions architect is searching for a one-time, highly available solution to this requirement that will also assist lower the number of IPs that the firewall must accept.

What recommendations should the solutions architect make to satisfy these requirements?

- A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions. Keep refreshing this list.
- B. Set up a Network Load Balancer (NLB) with Elastic IPs. Register the private IPs of all the ALBs as targets to this NLB.
- C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.
- D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

Correct Answer: C **Question #485****Topic 1**

A business is developing a payment application that must be very reliable even in the event of regional service outages. A solutions architect must provide a data storage solution that is readily replicable and deployable across several AWS Regions. Additionally, the application needs low-latency atomicity, consistency, isolation, and durability (ACID) transactions that must be accessible promptly for report generation. Additionally, the development team must use SQL.

Which data storage option satisfies these criteria?

- A. Amazon Aurora Global Database
- B. Amazon DynamoDB global tables
- C. Amazon S3 with cross-Region replication and Amazon Athena
- D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

Correct Answer: C **Question #486****Topic 1**

A business want to run a scalable web application on Amazon Web Services. The program will be accessible by people from all around the globe. Users of the application will be able to download and upload unique data in the gigabyte range. The development team is looking for an economical solution that minimizes upload and download latency and optimizes speed.

What actions should a solutions architect take to achieve this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: C **Reference:**

<https://aws.amazon.com/ec2/autoscaling/>

Question #487

Topic 1

A business's on-premises volume backup system has reached the end of its useful life. The organization wants to include AWS into a new backup solution and wishes to retain local access to all data while it is backed up on AWS. The organization want to guarantee that data backed up on AWS is moved automatically and securely.

Which solution satisfies these criteria?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Correct Answer: D 

Question #488

Topic 1

A business maintains an on-premises application that gathers and saves data on an on-premises NFS server. The firm just established a ten gigabit per second AWS Direct Connect connection. The company's on-site storage capacity is rapidly depleting. The organization wants to move application data from its on-premises environment to the AWS Cloud while preserving low-latency access to the data from the on-premises application.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.
- B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.
- C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.
- D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

Correct Answer: A 

Question #489**Topic 1**

In another Region, a business has constructed an isolated backup of its environment. The application is in warm standby mode and is protected by a load balancer (ALB). At the moment, failover is a manual operation that needs changing a DNS alias record to link to the secondary ALB in another Region.

What is the best way for a solutions architect to automate the failover process?

- A. Enable an ALB health check
- B. Enable an Amazon Route 53 health check.
- C. Create an CNAME record on Amazon Route 53 pointing to the ALB endpoint.
- D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

Correct Answer: C **Question #490****Topic 1**

A business has two AWS accounts: one for production and one for development. There are code modifications ready to be sent to the Production account from the Development account.

Only two senior developers on the development team need access to the Production account during the alpha phase. During the beta phase, more developers may need access to undertake testing.

What recommendations should a solutions architect make?

- A. Create two policy documents using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Give one IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account with the trust policy that specifies the Development account. Allow developers to assume the role.
- D. Create an IAM group in the Production account and add it as a principal in the trust policy that specifies the Production account. Add developers to the group.

Correct Answer: D **Question #491****Topic 1**

A solutions architect is tasked with the responsibility of migrating a Windows internet information services (IIS) web application to Amazon Web Services (AWS). Currently, the program depends on a file share stored on the user's network-attached storage (NAS). The solutions recommended transferring the IIS web servers to Amazon EC2 instances spread across several Availability Zones and linked to the storage solution, as well as creating an Elastic Load Balancer on the instances.

Which alternative to an on-premises file sharing is the MOST robust and durable?

- A. Migrate the file Share to Amazon RDS.
- B. Migrate the file Share to AWS Storage Gateway
- C. Migrate the file Share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

Correct Answer: C 

Question #492

Topic 1

A multinational conglomerate with operations in North America, Europe, and Asia is developing a new distributed application to improve its worldwide supply chain and manufacturing processes. Orders placed on a single continent should be accessible to all Regions in less than a second. The database should be capable to failover with a minimal Recovery Time Objective (RTO). The application's uptime is critical to ensuring that production does not suffer.

What recommendations should a solutions architect make?

- A. Use Amazon DynamoDB global tables.
- B. Use Amazon Aurora Global Database.
- C. Use Amazon RDS for MySQL with a cross-Region read replica.
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

Correct Answer: A 

Question #493

Topic 1

A solutions architect must host a high-performance computing (HPC) workload on Amazon Web Services (AWS). The workload will be dispersed over hundreds of Amazon EC2 instances and will need concurrent access to a shared file system in order to facilitate distributed processing of big datasets. Multiple instances of the same dataset will be accessible concurrently. The workload demands an access latency of less than 1 millisecond. Following completion of processing, engineers will need access to the dataset for manual postprocessing.

Which solution will satisfy these criteria?

- A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.
- B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.
- C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.
- D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Correct Answer: C 

Reference:

<https://jayendrapatil.com/aws-fsx-for-lustre/>

Question #494

Topic 1

A firm is building a mobile game that sends score updates to a backend processor and then publishes the results on a leaderboard. A solutions architect must develop a solution capable of handling high volumes of traffic, processing mobile game updates in the order in which they are received, and storing the processed changes in a highly accessible database. Additionally, the organization wishes to reduce the management cost associated with maintaining the solution.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

Correct Answer: D 

Question #495

Topic 1

A development team is working in collaboration with another business to produce an integrated product. The other firm requires access to an Amazon Simple Queue Service (Amazon SQS) queue stored in the account of the development team. The other corporation want to poll the queue without granting access to its own account.

How should a solutions architect manage SQS queue access?

- A. Create an instance profile that provides the other company access to the SQS queue.
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

Correct Answer: C 

Question #496

Topic 1

The website of a business is used to offer things to the general public. The site is hosted on Amazon EC2 instances that are part of an Auto Scaling group and protected by an Application Load Balancer (ALB). Additionally, an Amazon CloudFront distribution is available, and AWS WAF is utilized to guard against SQL injection attacks. The ALB is where the CloudFront distribution originates. Recent security log analysis identified an external malicious IP address that should be prevented from visiting the website.

What steps should a solutions architect take to safeguard an application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Correct Answer: B 

If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those IP addresses.

AWS Web Application Firewall (WAF)  Helps to protect your web applications from common application-layer exploits that can affect availability or consume excessive resources. As you can see in my post (New  AWS WAF), WAF allows you to use access control lists (ACLs), rules, and conditions that define acceptable or unacceptable requests or IP addresses. You can selectively allow or deny access to specific parts of your web application and you can also guard against various SQL injection attacks. We launched WAF with support for Amazon CloudFront.

Reference:

<https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-loadbalancers/>

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-ip-conditions.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-ip-conditions.html> <https://aws.amazon.com/blogs/aws/aws-web-application-firewall-waf-for-application-load-balancers/>

Question #497

Topic 1

An Amazon EC2 instance is created in a new VPC's private subnet. Although this subnet lacks outward internet connectivity, the EC2 instance requires the ability to obtain monthly security updates from a third-party vendor.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
- B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
- C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
- D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Correct Answer: A 

Question #498

Topic 1

A solutions architect is tasked with the responsibility of creating the architecture for a new online application. The application will be hosted on AWS Fargate containers with an Application Load Balancer (ALB) and a PostgreSQL database hosted on Amazon Aurora. The web application will largely do read-only operations on the database.

What should the solutions architect do to assure the website's scalability as traffic increases? (Select two.)

- A. Enable auto scaling on the ALB to scale the load balancer horizontally.
- B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.
- C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.
- D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.
- E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

Correct Answer: BE 

Question #499

Topic 1

A business has detected access requests from many dubious IP addresses. The security team determines that the requests originate from many IP addresses within the same CIDR range.

What recommendations should a solutions architect provide to the team?

- A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.
- B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.
- C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.
- D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

Correct Answer: C 

Question #500

Topic 1

A business has a build server that is part of an Auto Scaling group and often runs numerous Linux instances. For tasks and setups, the build server needs stable and mountable shared NFS storage.

What kind of storage should a solutions architect recommend?

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

Correct Answer: D 

Reference:

<https://aws.amazon.com/efs/>

Question #501

Topic 1

AWS-hosted applications make advantage of an Amazon Aurora Multi-AZ deployment for their database. When analyzing performance measurements, a solutions architect observed that database reads are using a significant amount of I/O and increasing delay to write requests to the database.

What should the solutions architect do to distinguish between read and write requests?

- A. Enable read-through caching on the Amazon Aurora database.
- B. Update the application to read from the Multi-AZ standby instance.
- C. Create a read replica and modify the application to use the appropriate endpoint.
- D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

Correct Answer: C 

Amazon RDS Read Replicas -

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as

Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source

DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance.

Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon

Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the online documentation.

Application servers Database server

Question #502

Topic 1

A business operates an automotive sales website and keeps its listings in an Amazon RDS database. When a car is sold, the listing is deleted from the website and the data is sent to other target systems.

What kind of design should a solutions architect suggest?

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

Correct Answer: A 

Question #503

Topic 1

A business wants to run a web application on AWS that communicates with a database contained inside a VPC. The application should have a high degree of availability.

What recommendations should a solutions architect make?

- A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.
- B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.
- C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.
- D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

Correct Answer: B 

Question #504

Topic 1

A software company is launching a new software-as-a-service (SaaS) solution that will be used by a large number of Amazon Web Services (AWS) customers. The service is hosted inside a Virtual Private Cloud (VPC) behind a Network Load Balancer. The software manufacturer want to give users with access to this service with as little administrative overhead as possible and without exposing the service to the public internet.

What actions should a solutions architect take to achieve this objective?

- A. Create a peering VPC connection from each user's VPC to the software vendor's VPC.
- B. Deploy a transit VPC in the software vendor's AWS account. Create a VPN connection with each user account.
- C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.
- D. Deploy a transit VPC in the software vendor's AWS account. Create an AWS Direct Connect connection with each user account.

Correct Answer: C 

Question #505

Topic 1

A business is developing a new online service that will be hosted on Amazon EC2 instances with the assistance of an Elastic Load Balancer. However, many online service clients can only communicate with IP addresses that have been whitelisted on their firewalls.

What should a solutions architect suggest to a customer in order to satisfy their needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

Correct Answer: A 

Question #506

Topic 1

The application running on Amazon EC2 instances requires access to an Amazon S3 bucket. Due to the sensitivity of the data, it cannot be sent via the internet.

What configuration should a solutions architect make for access?

- A. Create a private hosted zone using Amazon Route 53.
- B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.
- C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.
- D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

Correct Answer: B 

Question #507

Topic 1

A business is collaborating with a third-party vendor who needs write access to the business's Amazon Simple Queue Service (Amazon SQS) queue. The vendor has their own Amazon Web Services account.

What actions should a solutions architect take to ensure least privilege access is implemented?

- A. Update the permission policy on the SQS queue to give write access to the vendor's AWS account.
- B. Create an IAM user with write access to the SQS queue and share the credentials for the IAM user.
- C. Update AWS Resource Access Manager to provide write access to the SQS queue from the vendor's AWS account.
- D. Create a cross-account role with access to all SQS queues and use the vendor's AWS account in the trust document for the role.

Correct Answer: D 

Question #508

Topic 1

A solutions architect is tasked with the responsibility of building an architecture for a new application that demands low network latency and high network throughput across Amazon EC2 instances.

Which component of the architectural design should be included?

- A. An Auto Scaling group with Spot Instance types.
- B. A placement group using a cluster placement strategy.
- C. A placement group using a partition placement strategy.
- D. An Auto Scaling group with On-Demand instance types.

Correct Answer: B 

Question #509

Topic 1

A business operates a website that is hosted on Amazon EC2 instances spread across two Availability Zones. The organization anticipates traffic increases around certain holidays and wants to provide a consistent customer experience.

How can a solutions architect satisfy this criterion?

- A. Use step scaling.
- B. Use simple scaling.
- C. Use lifecycle hooks.
- D. Use scheduled scaling.

Correct Answer: D 

Question #510**Topic 1**

A business wants to enhance the availability and performance of its stateless UDP-based workload. The workload is spread across various AWS Regions using Amazon EC2 instances.

What should a solutions architect suggest as a means of achieving this?

- A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.
- B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.
- C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
- D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

Correct Answer: D **Question #511****Topic 1**

A business has a hybrid application that is hosted on a number of on-premises servers that all have static IP addresses. There is already a VPN in place that connects the VPC to the on-premises network. The corporation want to disperse TCP traffic for internet users among its on-premises servers.

What recommendations should a solutions architect make to provide a highly accessible and scalable solution?

- A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.
- B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.
- C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.
- D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

Correct Answer: A **Question #512****Topic 1**

A business requires that an Amazon S3 gateway endpoint accept traffic only from trusted buckets.

Which approach should a solutions architect use in order to fulfill this requirement?

- A. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's trusted VPCs.
- B. Create a bucket policy for each of the company's trusted S3 buckets that allows traffic only from the company's S3 gateway endpoint IDs.
- C. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that blocks access from any VPC other than the company's trusted VPCs.
- D. Create an S3 endpoint policy for each of the company's S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

Correct Answer: D 

Question #513

Topic 1

A business is utilizing Amazon Elastic Container Service (Amazon ECS) to host its application and want to assure high availability. The business needs to be able to update its application even if nodes in one Availability Zone are unavailable. The application is projected to get 100 requests per second, and each container job is capable of serving at least 60 requests per second. The organization configured Amazon ECS to use a rolling update deployment mode, with the minimum healthy percent parameter set to 50% and the maximum healthy percent parameter set to 100%.

Which task and availability zone configurations satisfy these requirements?

- A. Deploy the application across two Availability Zones, with one task in each Availability Zone.
- B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.
- C. Deploy the application across three Availability Zones, with one task in each Availability Zone.
- D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

Correct Answer: A 

Question #514

Topic 1

A financial services organization maintains a web application that is accessible to users in the United States and Europe. The program is divided into two tiers: a database layer and a web server layer. The database tier is comprised of a MySQL database that is physically located in us-east-1. Amazon Route 53 geoproximity routing is used to route traffic to the nearest Region's instances. According to a performance analysis of the system, European users are not obtaining the same degree of query performance as users in the United States.

Which improvements to the database layer should be made to increase performance?

- A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.
- B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.
- C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.
- D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

Correct Answer: D 

Topic 1 - Single Topic

Question #515

Topic 1

A solutions architect is developing a solution that will lead customers to a backup static error page in the event that the original website becomes inaccessible. The DNS records for the major website are housed on Amazon Route 53, with the domain referring to an Application Load Balancer (ALB).

Which configuration should the solutions architect use in order to fulfill the business's requirements while reducing modifications and infrastructure overhead?

- A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.
- D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

Correct Answer: B 

Active-passive failover -

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to

DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route

53 responds to DNS queries using the secondary record.

How Amazon Route 53 averts cascading failures

As a first defense against cascading failures, each request routing algorithm (such as weighted and failover) has a mode of last resort. In this special mode, when all records are considered unhealthy, the Route 53 algorithm reverts to considering all records healthy.

For example, if all instances of an application, on several hosts, are rejecting health check requests, Route 53 DNS servers will choose an answer anyway and return it rather than returning no DNS answer or returning an NXDOMAIN (non-existent domain) response. An application can respond to users but still fail health checks, so this provides some protection against misconfiguration.

Similarly, if an application is overloaded, and one out of three endpoints fails its health checks, so that it's excluded from Route 53 DNS responses, Route 53 distributes responses between the two remaining endpoints. If the remaining endpoints are unable to handle the additional load and they fail, Route 53 reverts to distributing requests to all three endpoints.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-problems.html>

Question #516

Topic 1

A business notices a rise in the cost of Amazon EC2 in its most recent bill. The billing team observes an anomaly in the vertical scaling of instance types for a few EC2 instances. A solutions architect should build a graph comparing the previous two months' EC2 charges and conduct an in-depth study to determine the core cause of the vertical scaling.

How should the solutions architect create data with the LEAST amount of operational overhead possible?

- A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
- B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
- C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
- D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>

Question #517

Topic 1

On AWS, a business hosts an online marketplace web application. During peak hours, the program serves hundreds of thousands of users. The business requires a scalable, near-real-time solution for sharing information about millions of financial transactions with various other internal systems. Additionally, transactions must be processed to remove sensitive data prior to being stored in a document database for fast retrieval.

What recommendations should a solutions architect make to satisfy these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
- D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Correct Answer: C 

Question #518

Topic 1

A business may have many AWS accounts for different departments. One of the departments would want to share an Amazon S3 bucket with the rest of the organization.

Which of the following solutions requires the LEAST amount of effort?

- A. Enable cross-account S3 replication for the bucket.
- B. Create a pre-signed URL for the bucket and share it with other departments.
- C. Set the S3 bucket policy to allow cross-account access to other departments.
- D. Create IAM users for each of the departments and configure a read-only IAM policy.

Correct Answer: C 

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html>

Question #519

Topic 1

A business hosts a web application on Amazon Web Services (AWS) utilizing a single Amazon EC2 instance that saves user-uploaded documents in an Amazon Elastic Block Store (Amazon EBS) volume. To improve scalability and availability, the organization replicated the architecture and deployed a second EC2 instance and EBS volume in a different Availability Zone, both of which were placed behind an Application Load Balancer. After this update was made, users claimed that each time they refreshed the page, they could view a portion of their papers but never all of them.

What should a solutions architect suggest to guarantee that users have access to all of their documents simultaneously?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents.
- C. Copy the data from both EBS volumes to Amazon Elastic File System (Amazon EFS). Modify the application to save new documents to Amazon Elastic File System (Amazon EFS).
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

Correct Answer: C 

Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and

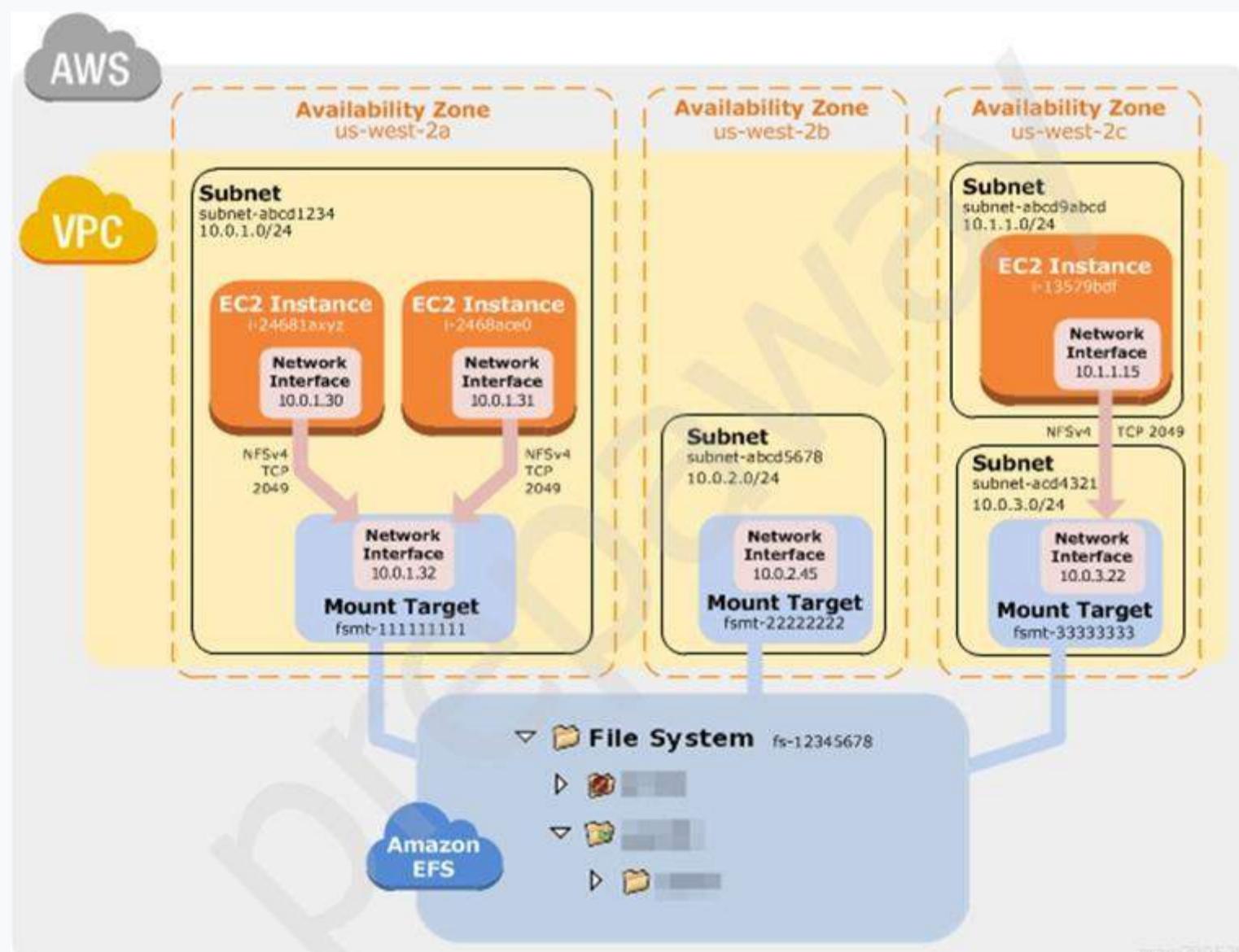
4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu

AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools.

For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For some AMIs, you'll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see Installing the NFS Client.

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

How Amazon EFS Works with Amazon EC2



Reference:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2>

Question #520*Topic 1*

A solutions architect is in the process of implementing a distributed database across many Amazon EC2 instances. The database replicates all data across numerous instances to ensure that it can survive the loss of single instance. The database needs block storage that is low in latency and high in throughput in order to accommodate several million transactions per second per server.

Which storage option should the architect of solutions use?

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

Correct Answer: *B* **Question #521***Topic 1*

A three-tier web application is used to handle client orders. The web tier is made up of Amazon EC2 instances behind an Application Load Balancer, a middle tier made up of three EC2 instances that are isolated from the web layer through Amazon SQS, and an Amazon DynamoDB backend. During busy periods, consumers who place purchases through the site must wait much longer than usual for confirmations owing to prolonged processing delays. A solutions architect's objective should be to minimize these processing times.

Which course of action will be the MOST EFFECTIVE in achieving this?

- A. Replace the SQS queue with Amazon Kinesis Data Firehose.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier.
- D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Correct Answer: *D* 

Question #522

Topic 1

A solutions architect is developing a solution that will need frequent modifications to a website hosted on Amazon S3 with versioning enabled. Due to compliance requirements, older versions of the objects will be seldom accessed and will need to be removed after two years.

What should the solutions architect propose as the CHEAPEST way to achieve these requirements?

- A. Use S3 batch operations to replace object tags. Expire the objects based on the modified tags.
- B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.
- C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SQS) queue for further processing.
- D. Replicate older object versions to a new bucket. Use an S3 Lifecycle policy to expire the objects in the new bucket after 2 years.

Correct Answer: B 

Question #523

Topic 1

A solutions architect is developing a web application that will be hosted on Amazon EC2 instances and managed by an Application Load Balancer (ALB). The organization places a high premium on the application's resilience to hostile internet activities and assaults, as well as its protection against newly discovered vulnerabilities and exposures.

What recommendations should the solutions architect make?

- A. Leverage Amazon CloudFront with the ALB endpoint as the origin.
- B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.
- C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.
- D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

Correct Answer: B 

Question #524

Topic 1

A business wishes to transition its online application to Amazon Web Services (AWS). The classic web application is divided into three tiers: the web layer, the application tier, and the MySQL database. The rearchitected application must be built using technologies that eliminate the need for the administration team to manage instances or clusters.

Which service combination should a solution architect include into the overall architecture? (Select two.)

- A. Amazon Aurora Serverless
- B. Amazon EC2 Spot Instances
- C. Amazon Elasticsearch Service (Amazon ES)
- D. Amazon RDS for MySQL
- E. AWS Fargate

Correct Answer: DE 

Question #525

Topic 1

A solutions architect is developing a security solution for a firm that want to deliver individual AWS accounts to developers through AWS Organizations while retaining normal security restrictions. Due to the fact that individual developers will have root user access to their own AWS accounts, the solutions architect needs to verify that the obligatory AWS CloudTrail configuration deployed to new developer accounts is not updated.

Which activity satisfies these criteria?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

Correct Answer: C 

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html

Question #526

Topic 1

A solutions architect is reviewing the security of a newly transferred workload. The workload is a web application that is composed of Amazon EC2 instances that are part of an Auto Scaling group and are routed via an Application Load Balancer. The solutions architect must strengthen the security posture and mitigate the resource effect of a DDoS assault.

Which of the following solutions is the MOST EFFECTIVE?

- A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.
- B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.
- C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.
- D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

Correct Answer: B 

Question #527

Topic 1

A business is building an ecommerce solution that will have a load-balanced front end, a container-based application, and a relational database. A solutions architect must design a highly accessible system that requires little human intervention.

Which solutions satisfy these criteria? (Select two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Correct Answer: AD 

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question #528

Topic 1

A business created a stateless two-tier application using Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ database instance. The new administration of the organization wants to guarantee that the application is highly accessible.

What actions should a solutions architect do in order to satisfy this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.
- D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

Correct Answer: A 

Question #529

Topic 1

A major company's administrator want to monitor and prevent cryptocurrency-related assaults on the company's AWS accounts.

Which AWS service can the administrator use to safeguard the organization from cyberattacks?

- A. Amazon Cognito
- B. Amazon GuardDuty
- C. Amazon Inspector
- D. Amazon Macie

Correct Answer: C 

Question #530

Topic 1

A business maintains data in an on-premises data center, which is utilized by a variety of on-premises applications. The organization wishes to preserve its current application environment while using AWS services for data analytics and future visualizations.

Which storage service should a solutions architect propose to his or her clients?

- A. Amazon Redshift
- B. AWS Storage Gateway for files
- C. Amazon Elastic Block Store (Amazon EBS)
- D. Amazon Elastic File System (Amazon EFS)

Correct Answer: B 

Question #531

Topic 1

A business is considering migrating a commercial off-the-shelf application from its on-premises data center to Amazon Web Services (AWS). The software is licensed on a per-socket and per-core basis, with predictable capacity and uptime requirements. The corporation wants to continue using its current licenses, which were acquired earlier this year.

Which price option for Amazon EC2 is the MOST cost-effective?

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

Correct Answer: C 

Question #532

Topic 1

A firm is developing a web application that will use Amazon S3 to store a big number of photos. Users will get access to the photographs for varying durations of time. The business wishes to:

- Retain all the images
- Incur no cost for retrieval.
- Have minimal management overhead.
- Have the images available with no impact on retrieval time.

Which solution satisfies these criteria?

- A. Implement S3 Intelligent-Tiering
- B. Implement S3 storage class analysis
- C. Implement an S3 Lifecycle policy to move data to S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Implement an S3 Lifecycle policy to move data to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A 

Question #533

Topic 1

On AWS Lambda, a corporation has created one of its microservices that connects to an Amazon DynamoDB database called Books. A solutions architect is creating an IAM policy that will be tied to the Lambda function's IAM role, granting it the ability to insert, edit, and remove objects from the Books table. The IAM policy must prohibit the function from doing any more activities on the Books or any other table.

Which IAM policy would meet these requirements while requiring the LEAST amount of privileged access?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        }  
    ]  
}
```

praw709528

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": [  
                "dynamodb: PutItem",  
                "dynamodb: UpdateItem",  
                "dynamodb: DeleteItem"  
            ],  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/*"  
        }  
    ]  
}
```

praw709528

C.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PutUpdateDeleteOnBooks",  
            "Effect": "Allow",  
            "Action": "dynamodb:*",  
            "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"  
        }  
    ]  
}
```

praw709528

D.



Correct Answer: A

Question #534

Topic 1

A business offers an online shopping application and all orders are stored in an Amazon RDS for PostgreSQL Single-AZ database instance. Management want to remove single points of failure and has requested a solutions architect to offer a method for minimizing database downtime without modifying the application code.

Which solution satisfies these criteria?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Correct Answer: A 

Question #535

Topic 1

A business intends to launch a freshly developed application on AWS in a default VPC. The program will be divided into two layers: a web layer and a database layer. The web server and MySQL database were constructed in public subnets, whereas the web server and MySQL database were created in private subnets. The default network ACL settings are used to build all subnets, and the default security group in the VPC is replaced with new custom security groups.

The critical criteria are as follows:

- The web servers must be accessible only to users on an SSL connection.
- The database should be accessible to the web layer, which is created in a public subnet only.
- All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of actions satisfies these criteria? (Select two.)

- A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0.0.0.0/0).
- B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.
- C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.
- D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.
- E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

Correct Answer: BD 

Question #536

Topic 1

A business wishes to enhance the availability and performance of a hybrid application. The application is composed of a stateful TCP-based workload that is hosted on Amazon EC2 instances across several AWS Regions, and a stateless UOP-based task that is housed on-premises.

Which activities should a solutions architect do in combination to increase availability and performance? (Select two.)

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

Correct Answer: AD 

Question #537

Topic 1

A corporation has recruited a new cloud engineer who should not have access to the CompanyConfidential Amazon S3 bucket. The cloud engineer must have read and write permissions on an S3 bucket named AdminTools.

Which IAM policy will satisfy these criteria?

A.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": "arn:aws:s3:::AdminTools"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

praw709528

B.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListBucket",  
            "Resource": [  
                "arn:aws:s3:::AdminTools",  
                "arn:aws:s3:::CompanyConfidential/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*"  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": "arn:aws:s3:::CompanyConfidential"  
        }  
    ]  
}
```

praw709528

C.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [ "s3:GetObject", "s3:PutObject" ],  
            "Resource": "arn:aws:s3:::AdminTools/*",  
        },  
        {  
            "Effect": "Deny",  
            "Action": "s3:*",  
            "Resource": [  
                "arn:aws:s3:::CompanyConfidential/*",  
                "arn:aws:s3:::CompanyConfidential"  
            ]  
        }  
    ]  
}
```

praw709528

D.
{

```
"Version": "2012-10-17",  
"Statement": [  
    {  
        "Effect": "Allow",  
        "Action": "s3>ListBucket",  
        "Resource": "arn:aws:s3:::AdminTools/*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": [ "s3:GetObject", "s3:PutObject", "s3>DeleteObject" ],  
        "Resource": "arn:aws:s3:::AdminTools/"  
    },  
    {  
        "Effect": "Deny",  
        "Action": "s3:*",  
        "Resource": [  
            "arn:aws:s3:::CompanyConfidential",  
            "arn:aws:s3:::CompanyConfidential/*",  
            "arn:aws:s3:::AdminTools/*"  
        ]  
    }  
]
```

praw709528

Correct Answer: C

Question #538

Topic 1

A business utilized an AWS Direct Connect connection to transfer one petabyte of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region. The business now wishes to replicate the data in another S3 bucket located in the us-west-2 Region.

Which solution will satisfy this criterion?

- A. Use an AWS Snowball Edge Storage Optimized device to copy the data from the colocation facility to us-west-2.
- B. Use the S3 console to copy the data from the source S3 bucket to the target S3 bucket.
- C. Use S3 Transfer Acceleration and the S3 copy-object command to copy the data from the source S3 bucket to the target S3 bucket.
- D. Add an S3 Cross-Region Replication configuration to copy the data from the source S3 bucket to the target S3 bucket.

Correct Answer: B 

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/move-objects-s3-bucket/>

Question #539

Topic 1

A business uses AWS to host a three-tier environment that collects sensor data from its consumers' devices. The traffic is routed via a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier and then to Amazon EC2 instances for the application layer that conducts database calls.

What should a solutions architect do to enhance data security when it is being sent to the web tier?

- A. Configure a TLS listener and add the server certificate on the NLB.
- B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

Correct Answer: C 

Question #540

Topic 1

A business is in the process of deploying a data lake on AWS. A solutions architect must describe a strategy for encrypting data at rest.

S3/Amazon According to the company's security policy:

- Keys must be rotated every 90 days.
- Strict separation of duties between key users and key administrators must be implemented.
- Auditing key usage must be possible.

What recommendations should the solutions architect make?

- A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)
- B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)
- C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)
- D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

Correct Answer: A 

Question #541

Topic 1

A business wishes to implement a shared file system for its .NET application servers and Microsoft SQL Server databases that are hosted on Amazon EC2 instances running Windows Server 2016. The solution must interact with the corporate Active Directory domain, be very durable, be managed by AWS, and provide high levels of throughput and IOPS.

Which solution satisfies these criteria?

- A. Use Amazon FSx for Windows File Server.
- B. Use Amazon Elastic File System (Amazon EFS).
- C. Use AWS Storage Gateway in file gateway mode.
- D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

Correct Answer: A 

AWS Certified Solutions Architect - Associate SAA-C02

Number: SAA-C02

Passing Score: 800

Time Limit: 120 min

File Version: 1

AWS Certified Solutions Architect - Associate SAA-C02

Exam A

QUESTION 1

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

- A. Launch the EC2 instances in a cluster placement group in one Availability Zone.
- B. Launch the EC2 instances in a spread placement group in one Availability Zone.
- C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
- D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/ec2/autoscaling/>

QUESTION 3

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

- A. Amazon EFS
- B. Amazon FSx
- C. Amazon S3
- D. AWS Storage Gateway

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

QUESTION 4

<https://www.vceoreteconvert.com/>

A company has a legacy application that process data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.

How should a solutions architect integrate the microservices?

- A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.
- B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.
- C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.
- D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Choose two.)

- A. Add AWS Shield.
- B. Add Aurora Replica.
- C. Add AWS Direct Connect.
- D. Add AWS Global Accelerator.
- E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

- A. Amazon EBS
- B. Amazon EC2 instance store
- C. Amazon EFS
- D. Amazon S3

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/ebs/>

QUESTION 9

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company's user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

- A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.
- B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.
- C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer

- endpoints in both Regions.
- D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

- A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.
- B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
- C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
- D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company's disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

- A. Create an additional S3 bucket in another Region and configure cross-Region replication.
- B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
- C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.
- D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://medium.com/@KerrySheldon/s3-exercise-2-4-adding-objects-to-an-s3-bucket-with->

[cross-region-replication-a78b332b7697](#)

QUESTION 12

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company's security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/>

QUESTION 13

A company's web application uses an Amazon RDS PostgreSQL DB instance to store its application data. During the financial closing period at the start of every month, Accountants run large queries that impact the database's performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

- A. Create a read replica and direct reporting traffic to the replica.
- B. Create a Multi-AZ database and direct reporting traffic to the standby.
- C. Create a cross-Region read replica and direct reporting traffic to the replica.
- D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

- A. Amazon S3 for cold data storage
- B. Amazon EFS for cold data storage
- C. Amazon S3 for high-performance parallel storage
- D. Amazon FSx for Lustre for high-performance parallel storage
- E. Amazon FSx for Windows for high-performance parallel storage

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solutions architect suggest?

- A. Set up an Amazon API Gateway and use Amazon ECS.
- B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
- C. Set up an Amazon API Gateway and use AWS Lambda functions.
- D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A solutions architect at an ecommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

- A. S3 Glacier
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. It's a good choice for storing secondary backup copies of on-premises data or easily re-creatable data. You can also use it as cost-effective storage for data that is replicated from another AWS Region using S3 Cross-Region Replication.

QUESTION 17

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

- A. Use Amazon SQS FIFO queues.
- B. Use an AWS Lambda function along with Amazon SQS standard queues.
- C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
- D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

QUESTION 18

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-purchase-options.html>

QUESTION 20

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution.

What should a solutions architect do to accomplish this?

- A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.
- B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage

- content. Configure Amazon CloudFront with the S3 bucket as the origin.
- C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.
 - D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- A. Create hourly snapshots of the production RDS DB instance.
- B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.
- C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.
- D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/blogs/database/best-storage-practices-for-running-production-workloads-on-hosted-databases-with-amazon-rds-or-amazon-ec2/>

QUESTION 22

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.

What is the MOST cost-effective solution?

- A. Amazon S3 Glacier
- B. Amazon S3 Standard
- C. Amazon S3 Intelligent-Tiering
- D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access

QUESTION 23

A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

- A. Purchase Reserved Instances to cover 250 instances.
- B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.
- C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.
- D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection.

What is the MOST cost-effective solution?

- A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket VPC endpoint.
- B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce VPC endpoint.
- C. Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to S3 objects to Amazon S3 Glacier.
- D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/s3/features/>

QUESTION 26

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster

experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

- A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.
- B. Use service control policies to disable IAM activity across all accounts in the organizational unit.
- C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
- D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

QUESTION 27

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

- A. Amazon RDS for MySQL
- B. Amazon RDS for PostgreSQL.
- C. Amazon ElastiCache for Redis
- D. Amazon ElastiCache for Memcached

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/elasticsearch/redis/faqs/>

QUESTION 29

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon

C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.

What should a solutions architect do to meet these requirements?

- A. Redesign the application to use Amazon CloudFront.
- B. Redesign the application to use AWS Elastic Beanstalk.
- C. Redesign the application to use a Network Load Balancer.
- D. Redesign the application to use Amazon S3 static website hosting.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

A-company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow.

Which solution meets these requirements?

- A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.
- B. Use a database in Amazon ROS with Multi-AZ and at least one standby replica.
- C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.
- D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

QUESTION 31

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```

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

```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region/
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand steaming?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html>

QUESTION 33

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
- C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 34**

A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

- A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
- B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.
- C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
- D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/efs/>

QUESTION 35

A company's managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



Amazon

SAA-C03

**AWS Certified Solutions Architect - Associate
QUESTION & ANSWERS**

QUESTION 1

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.

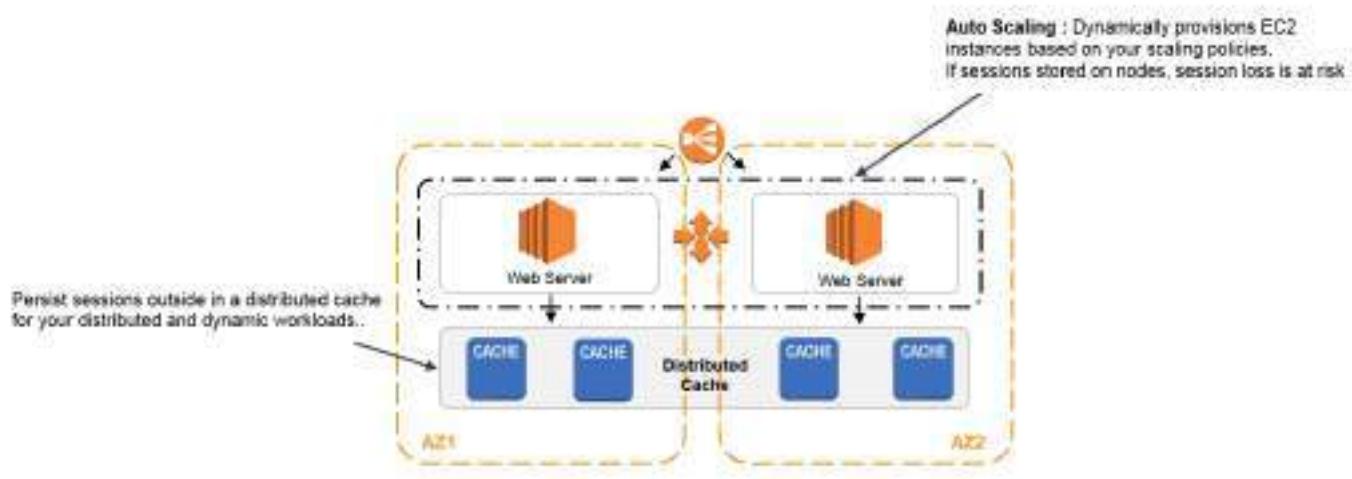
In this scenario, which AWS services are suitable for storing session state data? (Select TWO.)

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

Correct Answer: B,C

Explanation/Reference:

DynamoDB and ElastiCache are the correct answers. You can store session state data on both DynamoDB and ElastiCache. These AWS services provide high-performance storage of key-value pairs which can be used to build a highly available web application.



Redshift Spectrum is incorrect since this is a data warehousing solution where you can directly query data from your data warehouse. Redshift is not suitable for storing session state, but more on analytics and OLAP processes.

RDS is incorrect as well since this is a relational database solution of AWS. This relational storage type might not be the best fit for session states, and it might not provide the performance you need compared to DynamoDB for the same cost.

S3 Glacier is incorrect since this is a low-cost cloud storage service for data archiving and long-term backup. The archival and retrieval speeds of Glacier is too slow for handling session states.

References:

<https://aws.amazon.com/caching/database-caching/>
<https://aws.amazon.com/caching/session-management/>

Check out this Amazon Elasticache Cheat Sheet:
<https://tutorialsdojo.com/amazon-elasticache/>

QUESTION 2

A media company has an Amazon ECS Cluster, which uses the Fargate launch type, to host its news website. The application data are all stored in Amazon Keyspaces (for Apache Cassandra) with data-at-rest encryption enabled. 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. 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 Amazon Quantum Ledger Database (Amazon QLDB). Create an IAM role to the ECS task definition script that allows access to the Amazon QLDB and then pass the --cli-input-json parameter when calling the ECS register-task-definition action. Reference the task definition JSON file in the Amazon QLDB which contains the database credentials.
- B. Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS Certificate Manager (ACM). 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 ACM 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.
- C. 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 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. In the ECS task definition file of the ECS Cluster, store the database credentials to Amazon ECS Anywhere to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Allocate an IAM Role to the cluster to ensure that the passwords are only accessible by the ECS service tasks. Run the AWS IAM Access Analyzer to verify that the credentials can't be viewed in plaintext.

Correct Answer: C

Explanation/Reference:

Amazon ECS enables you to inject sensitive data into your containers by storing your sensitive data in either AWS Secrets Manager secrets or AWS Systems Manager Parameter Store parameters and then referencing them in your container definition. This feature is supported by tasks using both the EC2 and Fargate launch types.

Secrets can be exposed to a container in the following ways:

- To inject sensitive data into your containers as environment variables, use the secrets container definition parameter.

- To reference sensitive information in the log configuration of a container, use the container definition parameter.

The screenshot shows the AWS Systems Manager 'Create parameter' interface. The 'Parameter details' section includes a 'Name' field with the value 'databasepassword' and a 'Description' field with the value 'TutorialLab Shop Database Password'. Under the 'Tier' section, 'Standard' is selected. In the 'Type' section, 'String' is selected. Under 'KMS key source', 'My current account' is selected. A callout bubble points to 'SSM Parameter Value' which contains 'arn:aws:ssm:us-east-1:123456789012:parameter/databasepassword'. Another callout bubble points to 'KMS Parameter Key Encryption via AWS KMS'. The bottom right corner features a 'TUTORIALS DOJO' logo.

Within your container definition, specify secrets with the name of the environment variable to set in the container and the full ARN of either the Secrets Manager secret or Systems Manager Parameter Store parameter containing the sensitive data to present to the container. The parameter that you reference can be from a different Region than the container using it, but must be from within the same account.

Hence, the correct answer is the option that says: 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 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.

The option that says: In the ECS task definition file of the ECS Cluster, store the database credentials to Amazon ECS Anywhere to centrally manage these sensitive data and securely transmit it to only those containers that need access to it. Allocate an IAM Role to the cluster to ensure that the passwords are only accessible by the ECS service tasks. Run the AWS IAM Access Analyzer to verify that the credentials can't be viewed in plaintext is incorrect. Amazon Elastic Container Service (ECS) Anywhere is just a feature of Amazon ECS that enables you to easily run and manage container workloads on customer-managed infrastructure. This feature is not capable of storing any kind of credentials, let alone centrally manage your sensitive data. The recommended way to secure sensitive data in AWS is either through the use of Secrets Manager or Systems Manager Parameter Store. In addition, the AWS IAM Access Analyzer is primarily used to identify resources in your organization and accounts that are shared with an external entity, as well as to validate your IAM policies. This service can't verify if your database credentials are viewable in plaintext or not.

The option that says: 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 Amazon Quantum Ledger Database (Amazon QLDB). Create an IAM role to the ECS task definition script that allows access to the Amazon QLDB and then pass the --cli-input-json parameter when calling the ECS register-task-definition action. Reference the task definition JSON file in the Amazon QLDB which contains the database credentials is incorrect. Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. This service is not meant to store your sensitive database credentials.

The option that says: Use the AWS Secrets Manager to store the database credentials and then encrypt them using AWS Certificate Manager (ACM). 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 ACM 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 is incorrect. Although the use of Secrets Manager in securing sensitive data in ECS is valid, Amazon ECS doesn't support resource-based policies. An example of a resource-based policy is the S3 bucket policy. An ECS task assumes an execution role (IAM role) to be able to call other AWS services like AWS Secrets Manager on your behalf. In addition, you cannot encrypt database credentials using the AWS Certificate Manager (ACM) service. You have to use AWS KMS instead.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/specifying-sensitive-data.html>
<https://aws.amazon.com/blogs/mt/the-right-way-to-store-secrets-using-parameter-store/>
<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

Check out these Amazon ECS and AWS Systems Manager Cheat Sheets:

<https://tutorialsdojo.com/amazon-elastic-container-service-amazon-ecs/>
<https://tutorialsdojo.com/aws-systems-manager/>

QUESTION 3

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.)

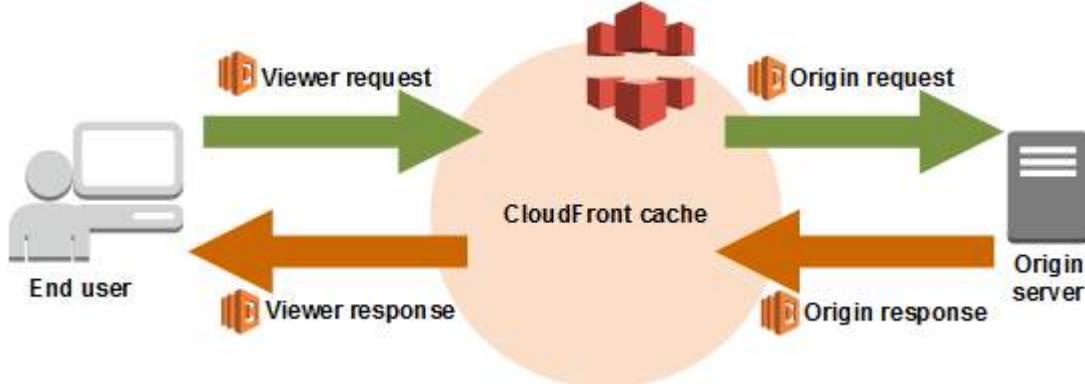
- A. Configure your origin to add a Cache-Control max-age directive to your objects, and specify the longest practical value for max-age to increase the cache hit ratio of your CloudFront distribution.
- B. Use multiple and geographically disperse VPCs to various AWS regions then create a transit VPC 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.
- C. 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.
- 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. 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.

Correct Answer: C,D

Explanation/Reference:

Lambda@Edge lets you run Lambda functions to customize the content that CloudFront delivers, executing the functions in AWS locations closer to the viewer. The functions run in response to CloudFront events, without provisioning or managing servers. You can use Lambda functions to change CloudFront requests and responses at the following points:

- After CloudFront receives a request from a viewer (viewer request)
- Before CloudFront forwards the request to the origin (origin request)
- After CloudFront receives the response from the origin (origin response)
- Before CloudFront forwards the response to the viewer (viewer response)



In the given scenario, you can use Lambda@Edge to allow your Lambda functions to customize the content that CloudFront delivers and to execute the authentication process in AWS locations closer to the users. In addition, you can set up an origin failover by creating an origin group with two origins with one as the primary origin and the other as the second origin which CloudFront automatically switches to when the primary origin fails. This will alleviate the occasional HTTP 504 errors that users are experiencing. Therefore, the correct answers are:

- 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.
- 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.

The option that says: 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 is incorrect because of the same reason provided above. Although setting up multiple VPCs across various regions which are connected with a transit VPC is valid, this solution still entails higher setup and maintenance costs. A more cost-effective option would be to use Lambda@Edge instead.

The option that says: 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 is incorrect because improving the cache hit ratio for the CloudFront distribution is irrelevant in this scenario. You can improve your cache performance by increasing the proportion of your viewer requests that are served from CloudFront edge caches instead of going to your origin servers for content. However, take note that the problem in the scenario is the sluggish authentication process of your global users and not just the caching of the static objects.

The option that says: 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 is incorrect. Although this may resolve the performance issue, this solution entails a significant implementation cost since you have to deploy your application to multiple AWS regions. Remember that the scenario asks for a solution that will improve the performance of the application with minimal cost.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_fallover.html

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html>

Check out these Amazon CloudFront and AWS Lambda Cheat Sheets:

<https://tutorialsdojo.com/amazon-cloudfront/>

<https://tutorialsdojo.com/aws-lambda/>

QUESTION 4

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

Correct Answer: D

Explanation/Reference:

In this scenario, the main culprit is that 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.

The option that says: The `sqsSendMessage` attribute of the SQS queue is configured to 50 is incorrect as there is no `sqsSendMessage` attribute in SQS.

The option that says: There is a bug in the application is a valid answer but since the scenario did not mention that the EC2 instances deleted the processed messages, the most likely cause of the problem is that the application does not issue a delete command to the SQS queue as mentioned above.

The option that says: 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 is incorrect as SQS does not automatically delete the messages.

Reference:

<https://aws.amazon.com/sqs/faqs/>

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

QUESTION 5

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?

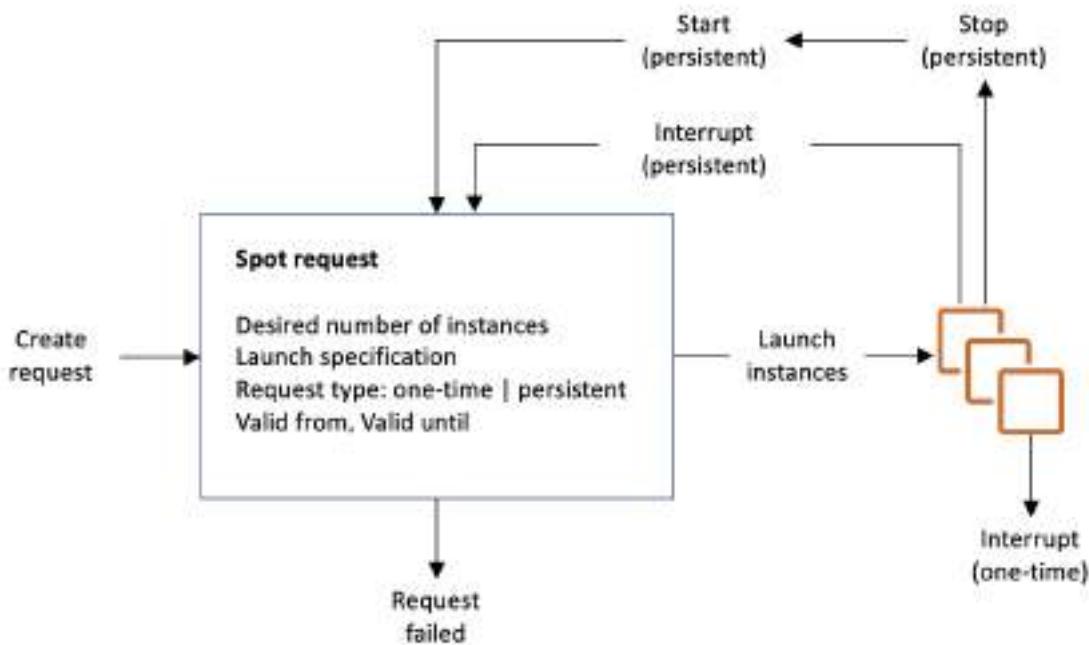
- A. Spot Instances
- B. Reserved Instances
- C. On-Demand Instances
- D. On-Demand Capacity Reservations

Correct Answer: A

Explanation/Reference:

Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. It can be interrupted by AWS EC2 with two minutes of notification when the EC2 needs the capacity back.

To use Spot Instances, you create a Spot Instance request that includes the number of instances, the instance type, the Availability Zone, and the maximum price that you are willing to pay per instance hour. If your maximum price exceeds the current Spot price, Amazon EC2 fulfills your request immediately if capacity is available. Otherwise, Amazon EC2 waits until your request can be fulfilled or until you cancel the request.



References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

<https://aws.amazon.com/ec2/spot/>

Amazon EC2 Overview:

https://youtu.be/7VsGIHT_jQE

Check out this Amazon EC2 Cheat Sheet:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

QUESTION 6

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. Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.
- B. It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator.
- C. It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
- D. Provides synchronous replication and automatic failover in the case of Availability Zone service failures.
- E. Allows both read and write operations on the read replica to complement the primary database.

Correct Answer: A,C

Explanation/Reference:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

For the MySQL, MariaDB, PostgreSQL, and Oracle database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for readscaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always spans at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

When you create a read replica for Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle, Amazon RDS sets up a secure communications channel using public-key encryption between the source DB instance and the read replica, even when replicating across regions. Amazon RDS establishes any AWS security configurations such as adding security group entries needed to enable the secure channel.

You can also create read replicas within a Region or between Regions for your Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle database instances encrypted at rest with AWS Key Management Service (KMS).

Hence, the correct answers are:

- It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
- Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.

The option that says: Allows both read and write operations on the read replica to complement the primary database is incorrect as Read Replicas are primarily used to offload read-only operations from the primary database instance. By default, you can't do a write operation to your Read Replica.

The option that says: Provides synchronous replication and automatic failover in the case of Availability Zone service failures is incorrect as this is a benefit of Multi-AZ and not of a Read Replica. Moreover, Read Replicas provide an asynchronous type of replication and not synchronous replication.

The option that says: It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator is incorrect because Read Replicas do not do anything to upgrade or increase the read throughput on the primary DB instance per se, but it provides a way for your application to fetch data from replicas. In this way, it improves the overall performance of your entire database-tier (and not just the primary DB instance). It doesn't increase the IOPS nor use AWS Global Accelerator to accelerate the compute capacity of your primary database. AWS Global Accelerator is a networking service, not related to RDS, that direct user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It simply routes the traffic to the closest edge location via Anycast.

References:

<https://aws.amazon.com/rds/details/read-relicas/>

<https://aws.amazon.com/rds/features/multi-az/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Additional tutorial - How do I make my RDS MySQL read replica writable?

<https://youtu.be/j5da6d2TIPc>

QUESTION 7

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

Correct Answer: B,D

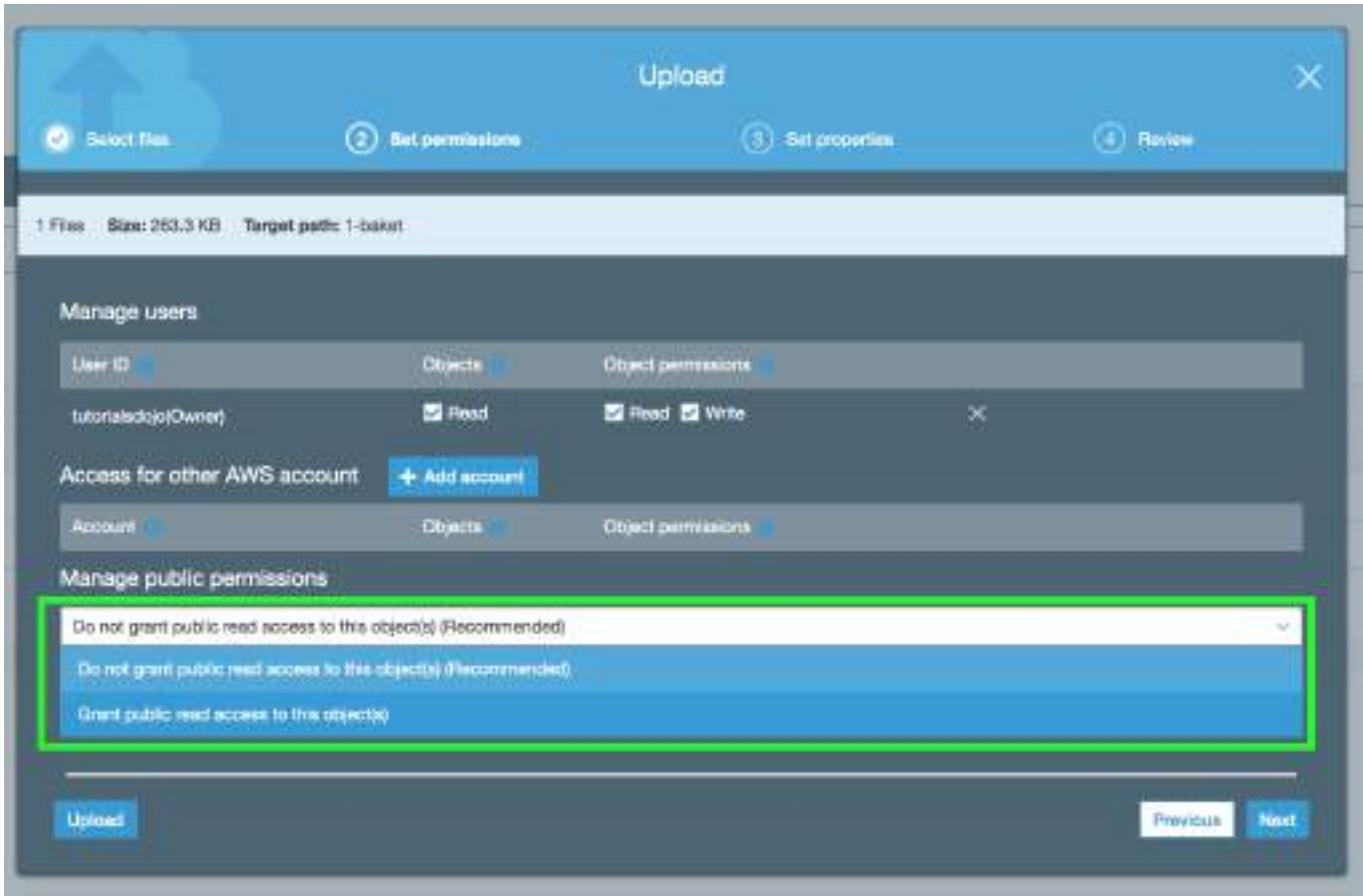
Explanation/Reference:

By default, all Amazon S3 resources such as buckets, objects, and related subresources are private which means that only the AWS account holder (resource owner) that created it has access to the resource. The resource owner can optionally grant access permissions to others by writing an access policy. In S3, you also set the permissions of the object during upload to make it public.

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies.

For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

You can also manage the public permissions of your objects during upload. Under Manage public permissions, you can grant read access to your objects to the general public (everyone in the world), for all of the files that you're uploading. Granting public read access is applicable to a small subset of use cases such as when buckets are used for websites.



Hence, the correct answers are:

- Grant public read access to the object when uploading it using the S3 Console.
- Configure the S3 bucket policy to set all objects to public read.

The option that says: Configure the cross-origin resource sharing (CORS) of the S3 bucket to allow objects to be publicly accessible from all domains is incorrect. CORS will only allow objects from one domain (travel.cebu.com) to be loaded and accessible to a different domain (palawan.com). It won't necessarily expose objects for public access all over the internet.

The option that says: Creating an IAM role to set the objects inside the S3 bucket to public read is incorrect. You can create an IAM role and attach it to an EC2 instance in order to retrieve objects from the S3 bucket or add new ones. An IAM Role, in itself, cannot directly make the S3 objects public or change the permissions of each individual object.

The option that says: Do nothing. Amazon S3 objects are already public by default is incorrect because, by default, all the S3 resources are private, so only the AWS account that created the resources can access them.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

QUESTION 8

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 RDS Read Replica of the production database. Direct the Data Analytics team to query the production data from the replica.
- C. 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.
- 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.

Correct Answer: B

Explanation/Reference:

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, Oracle and PostgreSQL, as well as Amazon Aurora.

Multi-AZ Deployments	Read Replicas
Synchronous replication – highly durable	Asynchronous replication – highly scalable
Only database engine on primary instance is active	All read replicas are accessible and can be used for read scaling
Automated backups are taken from standby	No backups configured by default
Always span two Availability Zones within a single Region	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Database engine version upgrades happen on primary	Database engine version upgrade is independent from source instance
Automatic failover to standby when a problem is detected	Can be manually promoted to a standalone database instance

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. These replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

Because read replicas can be promoted to master status, they are useful as part of a sharding implementation. To shard your database, add a read replica and promote it to master status, then, from each of the resulting DB Instances, delete the data that belongs to the other shard.

Hence, the correct answer is: 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.

The option that says: 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 is incorrect because Redshift is primarily used for OLAP (Online Analytical Processing) applications and not for OLTP.

The option that says: 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 is incorrect because you can't directly connect to the standby instance. This is only used in the event of a database failover when your primary instance encountered an outage.

The option that says: Upgrade the instance type of the RDS database to a large instance is incorrect because this entails a significant amount of cost. Moreover, the production database could still be affected by the queries done by the Data Analytics team. A better solution for this scenario is to use a Read Replica instead.

References:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/rds/details/read-replicas/>

<https://aws.amazon.com/elasticache/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

QUESTION 9

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?

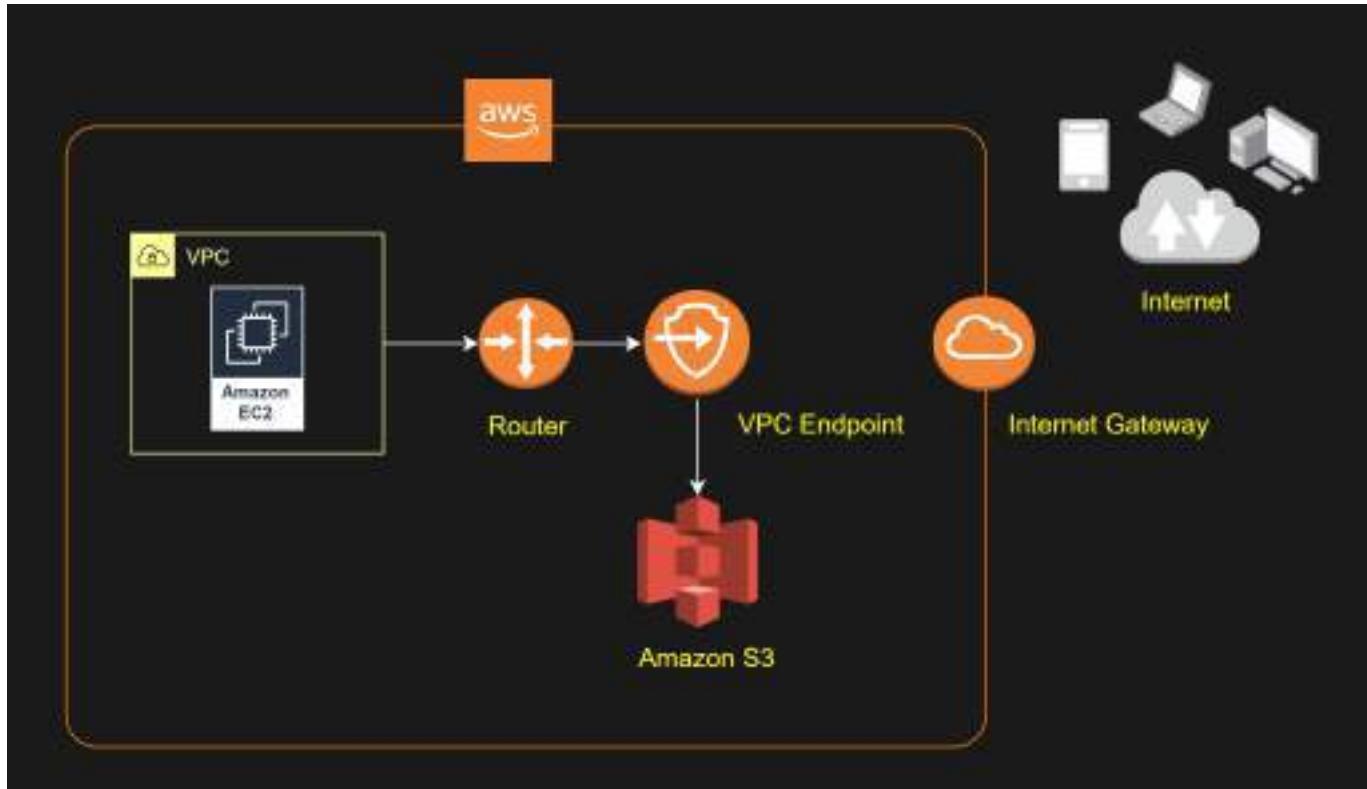
- A. Create an Amazon S3 interface endpoint to enable a connection between the instances and Amazon S3.
- B. Set up an AWS Transit Gateway to access Amazon S3.
- C. Create an Amazon S3 gateway endpoint to enable a connection between the instances and Amazon S3.
- D. Set up a NAT Gateway in the public subnet to connect to Amazon S3.

Correct Answer: C

Explanation/Reference:

VPC endpoints for Amazon S3 simplify access to S3 from within a VPC by providing configurable and highly reliable secure connections to S3 that do not require an internet gateway or Network Address Translation (NAT) device. When you create an S3 VPC endpoint, you can attach an endpoint policy to it that controls access to Amazon S3.

You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints. A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on-premises, or from a different AWS Region. Interface endpoints are compatible with gateway endpoints. If you have an existing gateway endpoint in the VPC, you can use both types of endpoints in the same VPC.



There is no additional charge for using gateway endpoints. However, standard charges for data transfer and resource usage still apply.

Hence, the correct answer is: Create an Amazon S3 gateway endpoint to enable a connection between the instances and Amazon S3.

The option that says: Set up a NAT Gateway in the public subnet to connect to Amazon S3 is incorrect. This will enable a connection between the private EC2 instances and Amazon S3 but it is not the most cost-efficient solution. NAT Gateways are charged on an hourly basis even for idle time.

The option that says: Create an Amazon S3 interface endpoint to enable a connection between the instances and Amazon S3 is incorrect. This is also a possible solution but it's not the most cost-effective solution. You pay an hourly rate for every provisioned Interface endpoint.

The option that says: Set up an AWS Transit Gateway to access Amazon S3 is incorrect because this service is mainly used for connecting VPCs and on-premises networks through a central hub.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

QUESTION 10

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 security group of the EC2 instance needs to be modified.
- B. The newly created VPC has an invalid CIDR block.
- C. The DNS resolution and DNS hostname of the VPC configuration should be enabled.
- D. Amazon Route53 is not enabled.

Correct Answer: C

Explanation/Reference:

When you launch an EC2 instance into a default VPC, AWS provides it with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

The screenshot shows the AWS VPC console. At the top, there is a table with columns: VPC ID, State, VPC CIDR, DHCP options set, and Route table. Two VPCs are listed:

VPC ID	State	VPC CIDR	DHCP options set	Route table
vpc-3902905c	available	172.31.0.0/16	dopt-fa2f3498	rtb-554ed530
vpc-d0bf29b4	available	10.10.0.0/16	dopt-fa2f3498	rtb-100d4174

Below the table, a section titled "PrivateSDN" is shown. It contains tabs for "Logs" and "Tags". Under "Logs", there is a table with the following information:

VPC ID	State	Network ACL
vpc-d0bf29b4 PrivateSDN	available	acl-70c55c14
C CIDR: 10.10.0.0/16		Default
ons set: dopt-fa2f3498		
e table: rtb-100d4174		

On the right side of the "Logs" table, there is a red oval highlighting the "DNS resolution: yes" and "DNS hostnames: yes" fields under the Network ACL section.

However, when you launch an instance into a non-default VPC, AWS provides the instance with a private DNS hostname only. New instances will only be provided with public DNS hostname depending on these two DNS attributes: the DNS resolution and DNS hostnames, that you have specified for your VPC, and if your instance has a public IPv4 address.

In this case, the new EC2 instance does not automatically get a DNS hostname because the DNS resolution and DNS hostnames attributes are disabled in the newly created VPC.

Hence, the correct answer is: The DNS resolution and DNS hostname of the VPC configuration should be enabled.

The option that says: The newly created VPC has an invalid CIDR block is incorrect since it's very unlikely that a VPC has an invalid CIDR block because of AWS validation schemes.

The option that says: Amazon Route 53 is not enabled is incorrect since Route 53 does not need to be enabled. Route 53 is the DNS service of AWS, but the VPC is the one that enables assigning of instance hostnames.

The option that says: The security group of the EC2 instance needs to be modified is incorrect since security groups are just firewalls for your instances. They filter traffic based on a set of security group rules.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html>

<https://aws.amazon.com/vpc/>

Amazon VPC Overview:

<https://www.youtube.com/watch?v=oIDHKeNxvQQ>

Check out this Amazon VPC Cheat Sheet:

<https://tutorialsdojo.com/amazon-vpc/>

QUESTION 11

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 CloudFront distribution and set the EC2 instance as the origin.
- C. Create a step scaling policy and configure an instance warm-up time condition.
- D. Create a Network Load Balancer with slow-start mode.

Correct Answer: C

Explanation/Reference:

Amazon EC2 Auto Scaling helps you maintain application availability and allows you to automatically add or remove EC2 instances according to conditions you define. You can use the fleet management features of EC2 Auto Scaling to maintain the health and availability of your fleet. You can also use the dynamic and predictive scaling features of EC2 Auto Scaling to add or remove EC2 instances.

Dynamic scaling responds to changing demand and predictive scaling automatically schedules the right number of EC2 instances based on predicted demand. Dynamic scaling and predictive scaling can be used together to scale faster.

AWS Services Search for services, features, marketplace products [Option+S] Tutorials Dojo N. Virginia

EC2 > Auto Scaling groups > TutorialsDojo-AutoScaling

Create scaling policy

Policy type: Step scaling

Scaling policy name: TutorialsDojo_Step_Scaling_Makati

CloudWatch alarm: StatusCheckFailed_Alarm_TutorialsDojo

Choose an alarm that can scale capacity whenever:

breaches the alarm threshold: StatusCheckFailed > 50 for 1 consecutive periods of 300 seconds for the metric dimensions:

InstanceId = i-029b2f4a3e6a25eef

Take the action:

Add step

1 Percent of group when 50 <= StatusCheckFailed < +infinity

Add step

Add capacity units in increments of at least 1 capacity units

Instances need: 300 seconds warm up before including in metric

Instance Warm Up Time

Cancel Create

Step scaling applies “step adjustments” which means you can set multiple actions to vary the scaling depending on the size of the alarm breach. When you create a step scaling policy, you can also specify the number of seconds that it takes for a newly launched instance to warm up.

Hence, the correct answer is: Create a step scaling policy and configure an instance warm-up time condition.

The option that says: Create a Network Load Balancer with slow start mode is incorrect because Network Load Balancer does not support slow start mode. If you need to enable slow start mode, you should use Application Load Balancer.

The option that says: Create a new launch template and upgrade the size of the instance is incorrect because a larger instance does not always improve the boot time. Instead of upgrading the instance, you should create a step scaling policy and add a warm-up time.

The option that says: Create a CloudFront distribution and set the EC2 instance as the origin is incorrect because this approach only resolves the traffic latency. Take note that the requirement in the scenario is to resolve the timeout issue and not the traffic latency.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

<https://aws.amazon.com/ec2/autoscaling/faqs/>

Check out these AWS Cheat Sheets:

<https://tutorialsdojo.com/aws-auto-scaling/>

<https://tutorialsdojo.com/step-scaling-vs-simple-scaling-policies-in-amazon-ec2/>

QUESTION 12

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application. Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected

Correct Answer: A

QUESTION 13

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 Organizations.
- C. Use AWS Control Tower to easily and securely share your resources with your AWS accounts.
- D. Consolidate all of the company's accounts using AWS ParallelCluster.
- E. Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.

Correct Answer: B,E

Explanation/Reference:

AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM.

Many organizations use multiple accounts to create administrative or billing isolation, and limit the impact of errors. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. You can create resources centrally in a multi-account environment, and use RAM to share those resources across accounts in three simple steps: create a Resource Share, specify resources, and specify accounts. RAM is available to you at no additional charge.

You can procure AWS resources centrally, and use RAM to share resources such as subnets or License Manager configurations with other accounts. This eliminates the need to provision duplicate resources in every account in a multi-account environment, reducing the operational overhead of managing those resources in every account.

AWS Organizations is an account management service that lets you consolidate multiple AWS accounts into an organization that you create and centrally manage. With Organizations, you can create member accounts and invite existing accounts to join your organization. You can organize those accounts into groups and attach policy-based controls.

Hence, the correct combination of options in this scenario is:

- Consolidate all of the company's accounts using AWS Organizations.
- Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.

The option that says: 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 is incorrect because although you can delegate access to resources that are in different AWS accounts using IAM, this process is extremely tedious and entails a lot of operational overhead since you have to manually set up cross-account access to each and every AWS account of the company. A better solution is to use AWS Resources Access Manager instead.

The option that says: Use AWS Control Tower to easily and securely share your resources with your AWS accounts is incorrect because AWS Control Tower simply offers the easiest way to set up and govern a new, secure, multi-account AWS environment. This is not the most suitable service to use to securely share your resources across AWS accounts or within your Organization. You have to use AWS Resources Access Manager (RAM) instead.

The option that says: Consolidate all of the company's accounts using AWS ParallelCluster is incorrect because AWS ParallelCluster is simply an AWS-supported open-source cluster management tool that makes it easy for you to deploy and manage High-Performance Computing (HPC) clusters on AWS. In this particular scenario, it is more appropriate to use AWS Organizations to consolidate all of your AWS accounts.

References:

<https://aws.amazon.com/ram/>

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

QUESTION 14

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored. Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C

QUESTION 15

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 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.
- C. 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.

- 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.

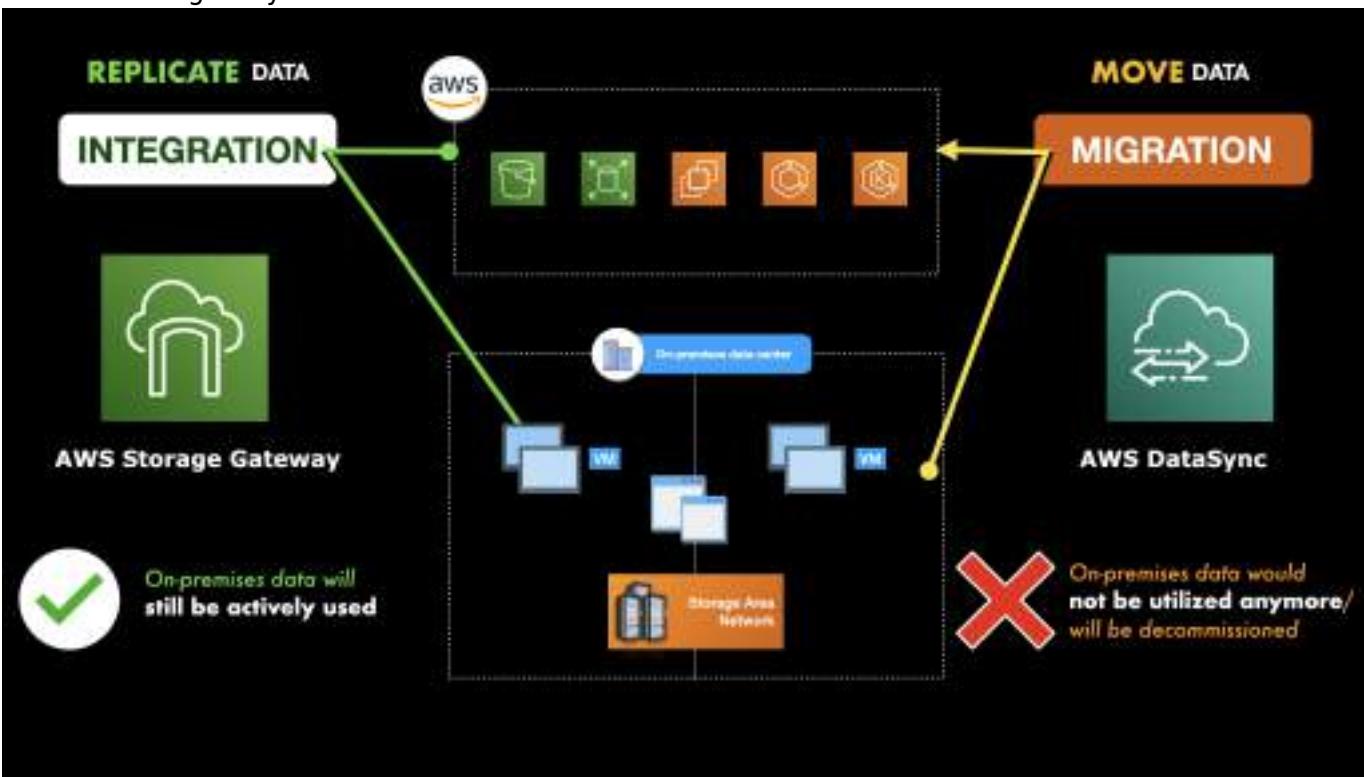
Correct Answer: C

Explanation/Reference:

AWS Storage Gateway is a set of hybrid cloud services that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to integrate AWS Cloud storage with existing on-site workloads so they can simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services. You can use DataSync to migrate active datasets to AWS, archive data to free up on-premises storage capacity, replicate data to AWS for business continuity, or transfer data to the cloud for analysis and processing.

Both AWS Storage Gateway and AWS DataSync can send data from your on-premises data center to AWS and vice versa. However, AWS Storage Gateway is more suitable to be used in integrating your storage services by replicating your data while AWS DataSync is better for workloads that require you to move or migrate your data.



You can also use a combination of DataSync and File Gateway to minimize your on-premises infrastructure while seamlessly connecting on-premises applications to your cloud storage. AWS DataSync enables you to automate and accelerate online data transfers to AWS storage services. File

Gateway is a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

There are two types of events that you configure your CloudTrail for:

- Management Events
- Data Events

Management Events provide visibility into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account.

Data Events, on the other hand, provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. It allows granular control of data event logging with advanced event selectors. You can currently log data events on different resource types such as Amazon S3 object-level API activity (e.g. GetObject, DeleteObject, and PutObject API operations), AWS Lambda function execution activity (the Invoke API), DynamoDB Item actions, and many more.

The screenshot shows the AWS S3 console. On the left, there's a sidebar with links like Buckets, Access Points, Object Lambda Access Points, Batch Operations, Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main area is titled 'Server access logging'. It has sections for 'Server access logging' (Enabled) and 'AWS CloudTrail data events (1)'. The 'AWS CloudTrail data events' section is highlighted with a green border. It contains a table with one row: Name (TutorialsDojo-Davao) and Access (Read, Write). Below this is an 'Event notifications (0)' section with a 'Create event notification' button. At the bottom, there are buttons for Edit, Delete, and Create event notification, along with columns for Name, Event types, Filters, and Des. typ.

With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help meet regulatory requirements that require WORM storage or to simply add another layer of protection against object changes and deletion.

Log properties	AWS CloudTrail	Amazon S3 server logs
Can be forwarded to other systems (CloudWatch Logs, CloudWatch Events)	Yes	
Deliver logs to more than one destination (for example, send the same logs to two different buckets)	Yes	
Turn on logs for a subset of objects (prefix)	Yes	
Cross-account log delivery (target and source bucket owned by different accounts)	Yes	
Integrity validation of log file using digital signatures/hashing	Yes	
Default choice of encryption for log files	Yes	
Object operations (using Amazon S3 API)	Yes	Yes
Bucket operations (using Amazon S3 API)	Yes	Yes
Searchable UI for logs	Yes	
Fields for Object Lock parameters, Amazon S3 Select properties for log records	Yes	
Fields for Object Size, Total Time, Turn-Around Time, and HTTP Referrer for log records		Yes
Lifecycle transitions, expirations, relocations		Yes
Logging of keys in a batch delete operation		Yes
Authentication failures ¹		Yes
Accounts where logs get delivered	Bucket owner ² , and requester	Bucket owner only

You can record the actions that are taken by users, roles, or AWS services on Amazon S3 resources and maintain log records for auditing and compliance purposes. To do this, you can use server access logging, AWS CloudTrail logging, or a combination of both. AWS recommends that you use AWS CloudTrail for logging bucket and object-level actions for your Amazon S3 resources.

Hence, the correct answer is: 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.

The option that says: 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 is incorrect. The requirement explicitly says that the Solutions Architect must immediately move the existing records to AWS and not integrate or replicate the data. Using AWS DataSync is a more suitable service to use here since the primary objective is to migrate or move data. You also have to use Data Events here and not Management Events in CloudTrail, to properly track all the data access and changes to your objects.

The option that says: 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 is incorrect. Just as mentioned in the previous option, using AWS Storage Gateway is not a recommended service to use in this situation since the objective is to move the obsolete data.

Moreover, using Amazon EBS to store health records is not a scalable solution compared with Amazon S3. Enabling server access logging can help audit the stored objects. However, it is better to use CloudTrail as it provides more granular access control and tracking.

The option that says: 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 is incorrect.

Although it is right to use AWS DataSync to move the health records, you still have to configure Data Events in AWS CloudTrail and not Management Events. This type of event only provides visibility into management operations that are performed on resources in your AWS account and not the data events that are happening in the individual objects in Amazon S3.

References:

- <https://aws.amazon.com/datasync/faqs/>
- <https://aws.amazon.com/about-aws/whats-new/2020/12/aws-cloudtrail-provides-more-granular-control-of-data-event-logging/>
- <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

Check out this AWS DataSync Cheat Sheet:
<https://tutorialsdojo.com/aws-datasync/>
AWS Storage Gateway vs DataSync:
<https://www.youtube.com/watch?v=tmfe1rO-AUs>

QUESTION 16

An online cryptocurrency exchange platform is hosted in AWS which uses ECS Cluster and RDS in Multi-AZ 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. Use Amazon CloudWatch to monitor the CPU Utilization of your database.
- D. Enable Enhanced Monitoring in RDS.

Correct Answer: D

Explanation/Reference:

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. By default, Enhanced Monitoring metrics are stored in the CloudWatch Logs for 30 days. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the CloudWatch console.

Take note that there are certain differences between CloudWatch and Enhanced Monitoring Metrics. CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. Hence, enabling Enhanced Monitoring in RDS is the correct answer in this specific scenario. The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Process List

 Filter process list

< 1 2 > 

NAME	VIRT	RES	CPU%	MEM%	VMLIMIT
▼ postgres [3181] 	283.55 MB	17.11 MB	0.02	1.72	
postgres:					
rdsadmin	384.7 MB	9.51 MB	0.02	0.95	
rdsadmin					
localhost(40156)					
idle [2953] 					

Using Amazon CloudWatch to monitor the CPU Utilization of your database is incorrect. Although you can use this to monitor the CPU Utilization of your database instance, it does not provide the percentage of the CPU bandwidth and total memory consumed by each database process in your RDS instance. Take note that CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance while RDS Enhanced Monitoring gathers its metrics from an agent on the instance.

The option that says: 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 is incorrect. Although you can use Amazon CloudWatch Logs and CloudWatch dashboard to monitor the CPU Utilization of the database instance, using CloudWatch alone is still not enough to get the specific percentage of the CPU bandwidth and total memory consumed by each database processes. The data provided by CloudWatch is not as detailed as compared with the Enhanced Monitoring feature in RDS. Take note as well that you do not have direct access to the instances/servers of your RDS database instance, unlike with your EC2 instances where you can install a CloudWatch agent or a custom script to get CPU and memory utilization of your instance.

The option that says: 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 is incorrect because the CPU% and MEM% metrics are not readily available in the Amazon RDS console, which is contrary to what is being stated in this option.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch>

Check out this Amazon CloudWatch Cheat Sheet:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

QUESTION 17

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.

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

What does the above IAM policy allow? (Select THREE.)

- A. An IAM user with this IAM policy is allowed to read and delete objects from the boracay S3 bucket.
- B. 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.
- C. An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
- 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 write objects into the boracay S3 bucket.
- F. An IAM user with this IAM policy is allowed to change access rights for the boracay S3 bucket.

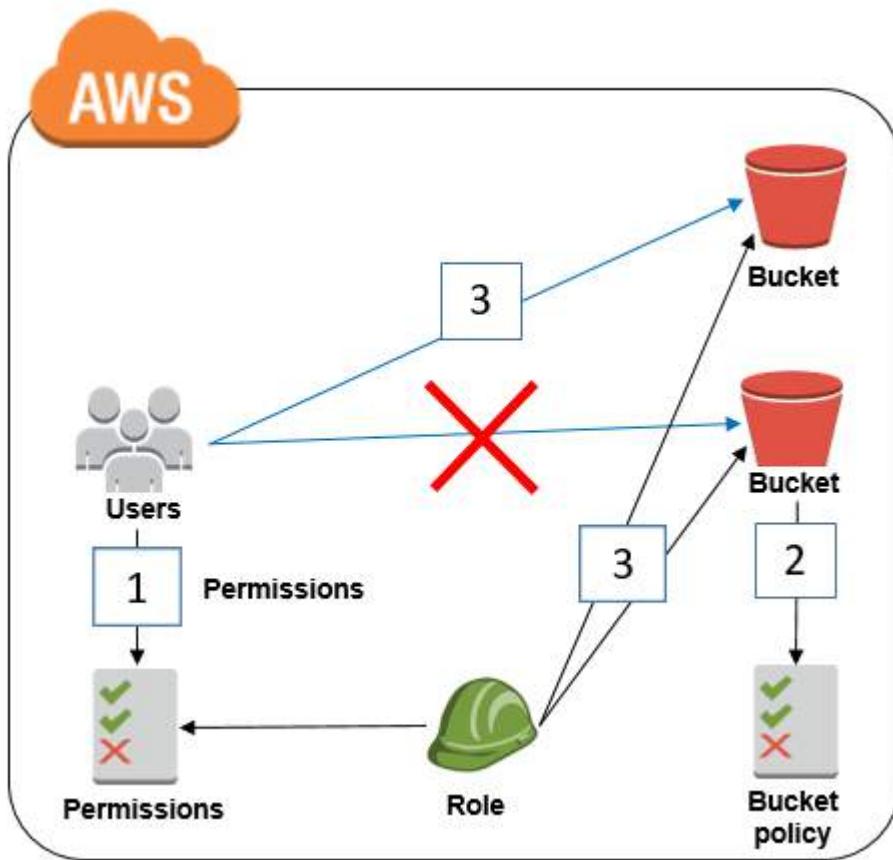
Correct Answer: C,D,E

Explanation/Reference:

You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, AWS Organizations SCPs, ACLs, and session policies.

IAM policies define permissions for action regardless of the method that you use to perform the operation. For example, if a policy allows the GetUser action, then a user with that policy can get user information from the AWS Management Console, the AWS CLI, or the AWS API. When you create an

IAM user, you can choose to allow console or programmatic access. If console access is allowed, the IAM user can sign in to the console using a user name and password. Or if programmatic access is allowed, the user can use access keys to work with the CLI or API.



Based on the provided IAM policy, the user is only allowed to get, write, and list all of the objects for the boracay s3 bucket. The s3:PutObject basically means that you can submit a PUT object request to the S3 bucket to store data.

Hence, the correct answers are:

- An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
- An IAM user with this IAM policy is allowed to write objects into the boracay S3 bucket.
- An IAM user with this IAM policy is allowed to read objects from the boracay S3 bucket.

The option that says: An IAM user with this IAM policy is allowed to change access rights for the boracay S3 bucket is incorrect because the template does not have any statements which allow the user to change access rights in the bucket.

The option that says: 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 is incorrect because it can clearly be seen in the template that there is a s3>List* which permits the user to list objects.

The option that says: An IAM user with this IAM policy is allowed to read and delete objects from the boracay S3 bucket is incorrect. Although you can read objects from the bucket, you cannot delete any objects.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectOps.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

QUESTION 18

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. AWS X-Ray
- D. Amazon CloudWatch

Correct Answer: B

Explanation/Reference:

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Amazon CloudWatch is incorrect because this is primarily used for systems monitoring based on the server metrics. It does not have the capability to track API calls to your AWS resources.

AWS X-Ray is incorrect because this is usually used to debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance. Unlike CloudTrail, it does not record the API calls that were made to your AWS resources.

Amazon API Gateway is incorrect because this is not used for logging each and every API call to your AWS resources. It is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Reference:

<https://aws.amazon.com/cloudtrail/>

Check out this AWS CloudTrail Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudtrail/>

QUESTION 19

A social media company needs to capture the detailed information of all HTTP requests that went through their public-facing Application Load Balancer every five minutes. The client's IP address and network latencies must also be tracked. They want to use this data for analyzing traffic patterns and for troubleshooting their Docker applications orchestrated by the Amazon ECS Anywhere service.

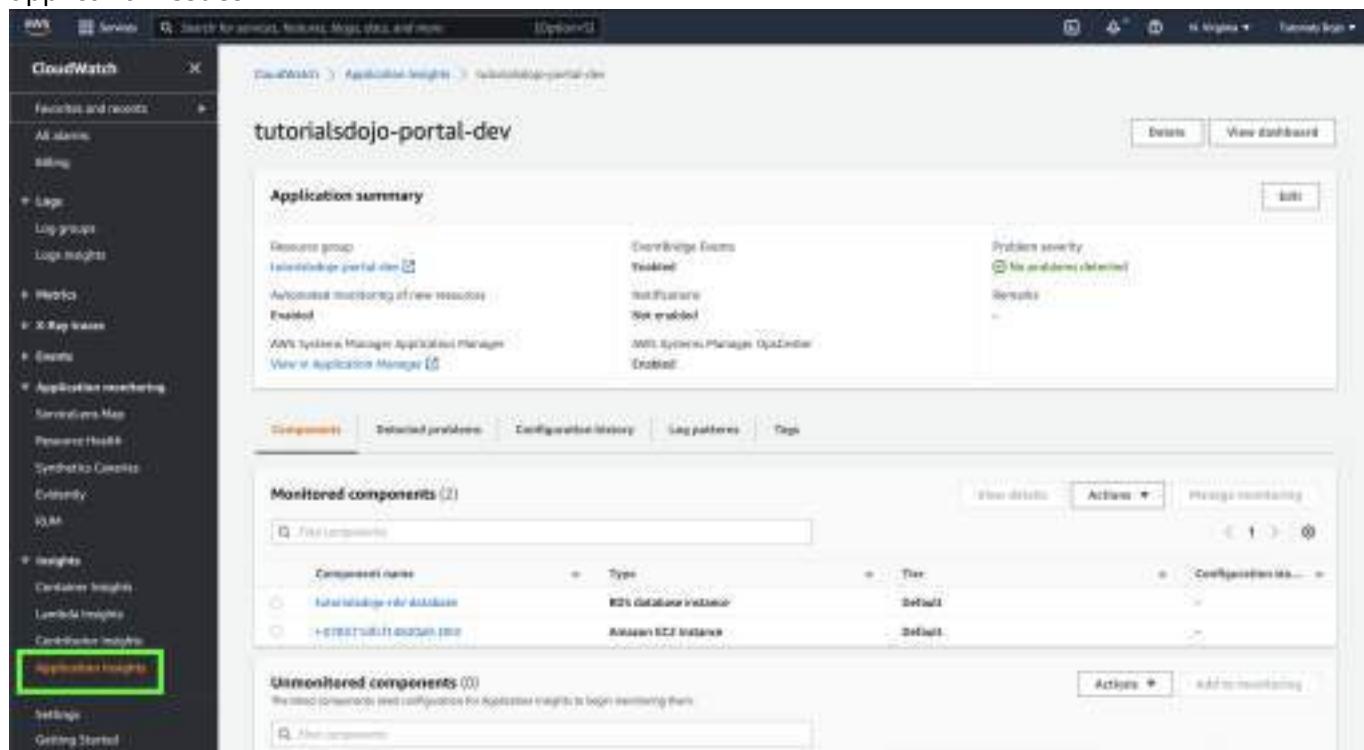
Which of the following options meets the customer requirements with the LEAST amount of overhead?

- A. Enable AWS CloudTrail for their Application Load Balancer. Use the AWS CloudTrail Lake to analyze and troubleshoot the application traffic.
- B. Enable access logs on the Application Load Balancer. Integrate the Amazon ECS cluster with Amazon CloudWatch Application Insights to analyze traffic patterns and simplify troubleshooting.
- C. Integrate Amazon EventBridge (Amazon CloudWatch Events) metrics on the Application Load Balancer to capture the client IP address. Use Amazon CloudWatch Container Insights to analyze traffic patterns.
- D. Install and run the AWS X-Ray daemon on the Amazon ECS cluster. Use the Amazon CloudWatch ServiceLens to analyze the traffic that goes through the application.

Correct Answer: B

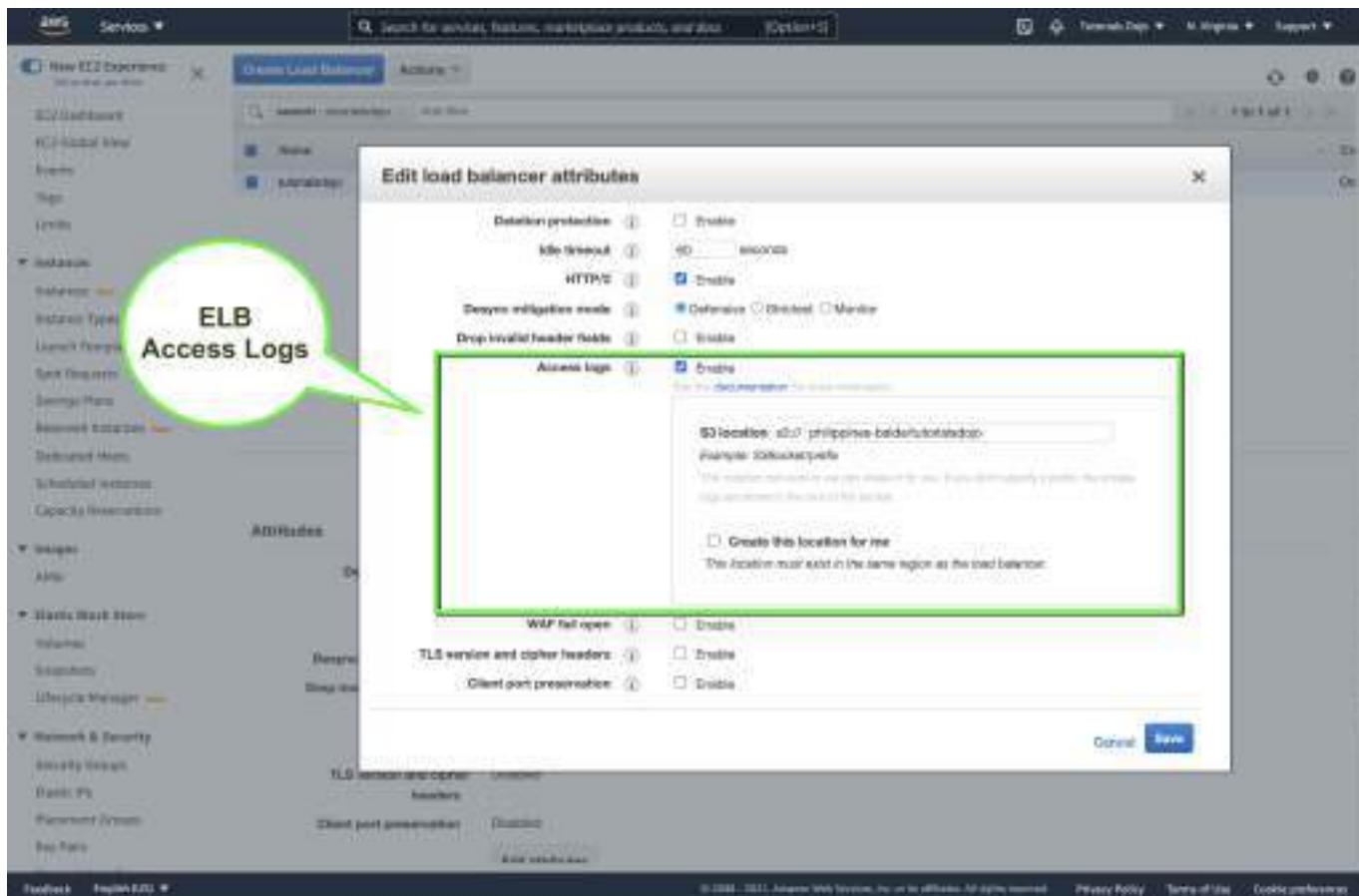
Explanation/Reference:

Amazon CloudWatch Application Insights facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications. Application Insights, which is powered by SageMaker and other AWS technologies, provides automated dashboards that show potential problems with monitored applications, which help you to quickly isolate ongoing issues with your applications and infrastructure. The enhanced visibility into the health of your applications that Application Insights provides helps reduce the "mean time to repair" (MTTR) to troubleshoot your application issues.



When you add your applications to Amazon CloudWatch Application Insights, it scans the resources in the applications and recommends and configures metrics and logs on CloudWatch for application components. Example application components include SQL Server backend databases and Microsoft IIS/Web tiers. Application Insights analyzes metric patterns using historical data to detect anomalies and continuously detects errors and exceptions from your application, operating system, and infrastructure logs. It correlates these observations using a combination of classification algorithms and built-in rules. Then, it automatically creates dashboards that show the relevant observations and problem severity information to help you prioritize your actions.

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.



Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.

Hence, the correct answer is: Enable access logs on the Application Load Balancer. Integrate the Amazon ECS cluster with Amazon CloudWatch Application Insights to analyze traffic patterns and simplify troubleshooting.

The option that says: Enable AWS CloudTrail for their Application Load Balancer. Use the AWS CloudTrail Lake to analyze and troubleshoot the application traffic is incorrect because AWS CloudTrail is primarily used to monitor and record the account activity across your AWS resources and not your web applications. You cannot use CloudTrail to capture the detailed information of all HTTP requests that go through your public-facing Application Load Balancer (ALB). CloudTrail can only track the resource changes made to your ALB, but not the actual IP traffic that goes through it. For this use case, you have to enable the access logs feature instead. In addition, the AWS CloudTrail Lake feature is more suitable for running SQL-based queries on your API events and not for analyzing application traffic.

The option that says: Install and run the AWS X-Ray daemon on the Amazon ECS cluster. Use the Amazon CloudWatch ServiceLens to analyze the traffic that goes through the application is incorrect. Although this solution is possible, this won't track the client's IP address since the access log feature in the ALB is not enabled. Take note that the scenario explicitly mentioned that the client's IP address and network latencies must also be tracked.

The option that says: Integrate Amazon EventBridge (Amazon CloudWatch Events) metrics on the Application Load Balancer to capture the client IP address. Use Amazon CloudWatch Container Insights to analyze traffic patterns is incorrect because Amazon EventBridge doesn't track the actual traffic to your ALB. It is the Amazon CloudWatch service that monitors the changes to your ALB itself and the actual IP traffic that it distributes to the target groups. The primary function of CloudWatch Container Insights is to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-application-insights.html>

<http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-monitoring.html>

AWS Elastic Load Balancing Overview:

<https://youtu.be/UBI5dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

Application Load Balancer vs Network Load Balancer vs Gateway Load Balancer:

<https://tutorialsdojo.com/application-load-balancer-vs-network-load-balancer-vs-classic-load-balancer/>

QUESTION 20

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available. Which combination of configuration options will meet these requirements? (Choose two.)

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: C,E

QUESTION 21

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms. What should the solutions architect do to meet these requirements?

- A. Create Amazon CloudWatch composite alarms where possible
- B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
- C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm
- D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible

Correct Answer: A

QUESTION 22

A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability. Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages
- B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

Correct Answer: A

QUESTION 23

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

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

Correct Answer: C

QUESTION 24

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 be optionally stored in CloudTrail or in CloudWatch Logs.
- 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 only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk.

Correct Answer: B

Explanation/Reference:

AWS Elastic Beanstalk stores your application files and optionally, server log files in Amazon S3. If you are using the AWS Management Console, the AWS Toolkit for Visual Studio, or AWS Toolkit for Eclipse, an Amazon S3 bucket will be created in your account and the files you upload will be automatically copied from your local client to Amazon S3. Optionally, you may configure Elastic Beanstalk to copy your server log files every hour to Amazon S3. You do this by editing the environment configuration settings.

Thus, the correct answer is the option that says: Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs.

With CloudWatch Logs, you can monitor and archive your Elastic Beanstalk application, system, and custom log files from Amazon EC2 instances of your environments. You can also configure alarms that make it easier for you to react to specific log stream events that your metric filters extract. The CloudWatch Logs agent installed on each Amazon EC2 instance in your environment publishes metric data points to the CloudWatch service for each log group you configure. Each log group applies its own filter patterns to determine what log stream events to send to CloudWatch as data points. Log streams that belong to the same log group share the same retention, monitoring, and access control settings. You can configure Elastic Beanstalk to automatically stream logs to the CloudWatch service. The option that says: 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 is incorrect because the server log files can also be stored in either S3 or CloudWatch Logs, and not only on the EBS volumes of the EC2 instances which are launched by AWS Elastic Beanstalk.

The option that says: Application files are stored in S3. The server log files can be stored directly in

Glacier or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to Glacier. You can create a lifecycle policy to the S3 bucket to store the server logs and archive it in Glacier, but there is no direct way of storing the server logs to Glacier using Elastic Beanstalk unless you do it programmatically.

The option that says: Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to CloudTrail as this service is primarily used for auditing API calls.

Reference:

<https://aws.amazon.com/elasticbeanstalk/faqs/>

AWS Elastic Beanstalk Overview:

<https://www.youtube.com/watch?v=rx7e7Fej1Oo>

Check out this AWS Elastic Beanstalk Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-beanstalk/>

QUESTION 25

A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs.

What should a solutions architect do to meet these requirements?

- A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.
- B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.
- C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
- D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules.

Correct Answer: D

QUESTION 26

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 Conditions section is missing.
- B. The Resources 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.

Correct Answer: B

Explanation/Reference:

In CloudFormation, a template is a JSON or a YAML-formatted text file that describes your AWS infrastructure. Templates include several major sections. The Resources section is the only required section. Some sections in a template can be in any order. However, as you build your template, it might be helpful to use the logical ordering of the following list, as values in one section might refer to values from a previous section. Take note that all of the sections here are optional, except for Resources, which is the only one required.

- Format Version
- Description
- Metadata
- Parameters
- Mappings
- Conditions
- Transform
- Resources (required)
- Outputs

Reference:

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html>

Check out this AWS CloudFormation Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation - Templates, Stacks, Change Sets:
<https://www.youtube.com/watch?v=9Xpuprxg7aY>

QUESTION 27

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. Modify the DB instance settings and enable storage autoscaling.
- B. Increase the allocated storage for the DB instance.
- C. Change the default_storage_engine of the DB instance's parameter group to MyISAM.
- D. Modify the DB instance storage type to Provisioned IOPS.

Correct Answer: A

Explanation/Reference:

RDS Storage Auto Scaling automatically scales storage capacity in response to growing database workloads, with zero downtime.

Under-provisioning could result in application downtime, and over-provisioning could result in underutilized resources and higher costs. With RDS Storage Auto Scaling, you simply set your desired maximum storage limit, and Auto Scaling takes care of the rest.

RDS Storage Auto Scaling continuously monitors actual storage consumption, and scales capacity up automatically when actual utilization approaches provisioned storage capacity. Auto Scaling works with new and existing database instances. You can enable Auto Scaling with just a few clicks in the AWS Management Console. There is no additional cost for RDS Storage Auto Scaling. You pay only for the RDS resources needed to run your applications.

Hence, the correct answer is: Modify the DB instance settings and enable storage autoscaling.

The option that says: Increase the allocated storage for the DB instance is incorrect. Although this will solve the problem of low disk space, increasing the allocated storage might cause performance degradation during the change.

The option that says: Change the default_storage_engine of the DB instance's parameter group to MyISAM is incorrect. This is just a storage engine for MySQL. It won't increase the disk space in any way.

The option that says: Modify the DB instance storage type to Provisioned IOPS is incorrect. This may improve disk performance but it won't solve the problem of low database storage.

References:

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling

Check out this Amazon RDS Cheat Sheet:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

QUESTION 28

A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance. The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability. Which solution will meet these requirements?

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

Correct Answer: C

QUESTION 29

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.

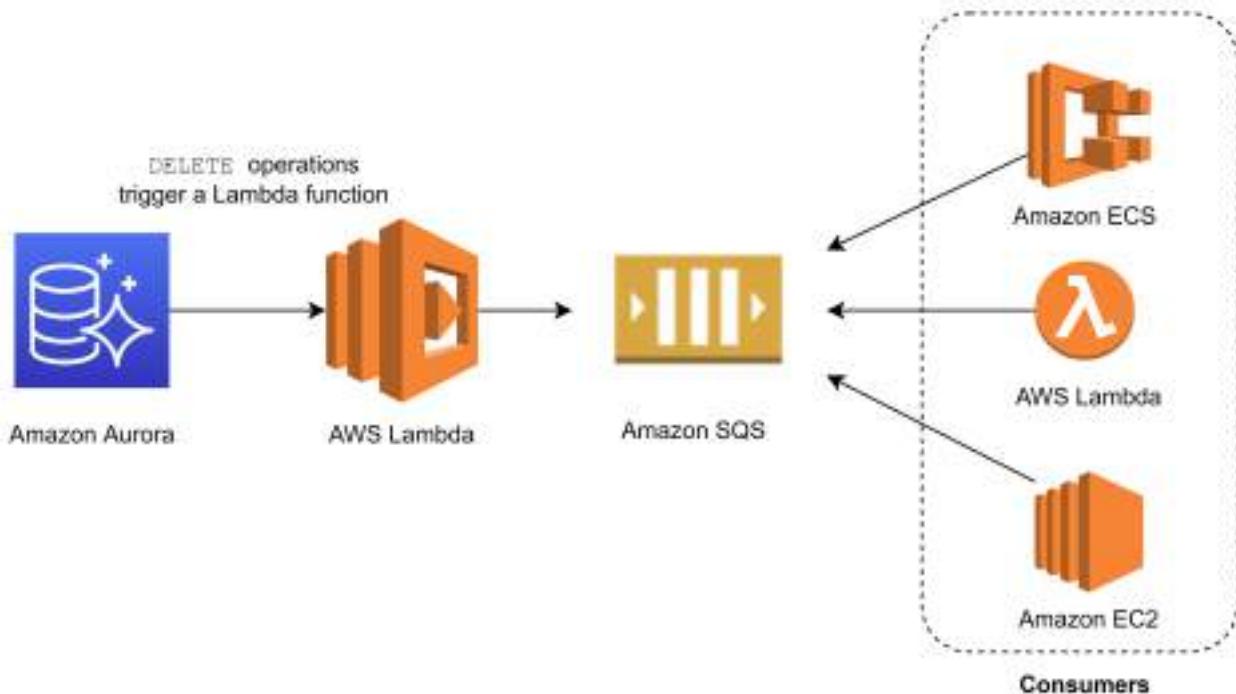
Which of the following options can satisfy the given requirement?

- A. Create 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.
- B. 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.
- C. 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.
- D. 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.

Correct Answer: A

Explanation/Reference:

You can invoke an AWS Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with a native function or a stored procedure. This approach can be useful when you want to integrate your database running on Aurora MySQL with other AWS services. For example, you might want to capture data changes whenever a row in a table is modified in your database.



In the scenario, you can trigger a Lambda function whenever a listing is deleted from the database. You can then write the logic of the function to send the listing data to an SQS queue and have different processes consume it.

Hence, the correct answer is: 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.

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures. Hence, the following options are incorrect:

- 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.
- 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.
- 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.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html>

<https://aws.amazon.com/blogs/database/capturing-data-changes-in-amazon-aurora-using-aws-lambda/>

Amazon Aurora Overview:

<https://youtu.be/iwS1h7rLNBQ>

Check out this Amazon Aurora Cheat Sheet:

<https://tutorialsdojo.com/amazon-aurora/>

QUESTION 30

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.

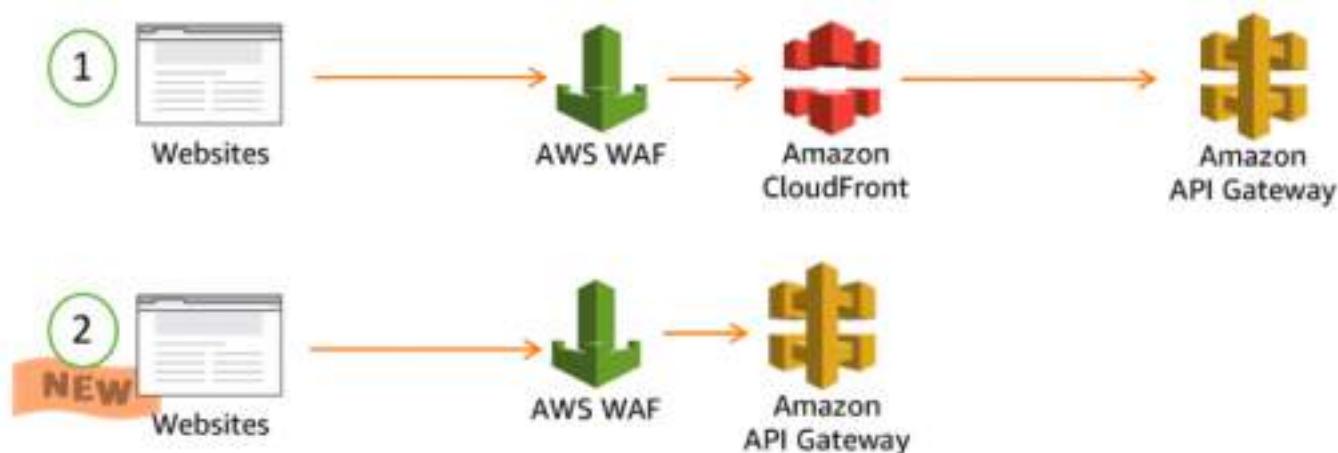
Which of the following should the Architect implement to mitigate this kind of attack?

- A. Block all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List.
- B. Use Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application.
- C. 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.
- D. 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.

Correct Answer: D

Explanation/Reference:

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, API Gateway, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You also can configure CloudFront to return a custom error page when a request is blocked.



At the simplest level, AWS WAF lets you choose one of the following behaviors:

Allow all requests except the ones that you specify - This is useful when you want CloudFront or an Application Load Balancer to serve content for a public website, but you also want to block requests

from attackers.

Block all requests except the ones that you specify – This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.

Count the requests that match the properties that you specify – When you want to allow or block requests based on new properties in web requests, you first can configure AWS WAF to count the requests that match those properties without allowing or blocking those requests. This lets you confirm that you didn't accidentally configure AWS WAF to block all the traffic to your website. When you're confident that you specified the correct properties, you can change the behavior to allow or block requests.

Hence, the correct answer in this scenario is: 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.

Using Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application is incorrect because Amazon GuardDuty is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Using AWS Firewall Manager to set up security rules that block SQL injection and cross-site scripting attacks, then associating the rules to the Application Load Balancer is incorrect because AWS Firewall Manager just simplifies your AWS WAF and AWS Shield Advanced administration and maintenance tasks across multiple accounts and resources.

Blocking all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List is incorrect because this is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. NACLs are not effective in blocking SQL injection and cross-site scripting attacks

References:

<https://aws.amazon.com/waf/>

<https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

Check out this AWS WAF Cheat Sheet:

<https://tutorialsdojo.com/aws-waf/>

AWS Security Services Overview - WAF, Shield, CloudHSM, KMS:

<https://www.youtube.com/watch?v=-1S-RdeAmMo>

QUESTION 31

A company has a UAT and production EC2 instances running on AWS. They want to ensure that employees who are responsible for the UAT instances don't have the access to work on the production instances to minimize security risks.

Which of the following would be the best way to achieve this?

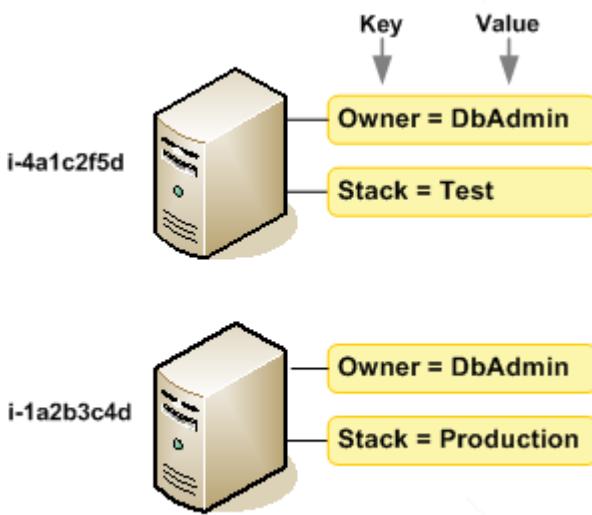
- A. Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication.
- B. Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that are used for production or development.
- C. Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.
- D. Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering.

Correct Answer: C

Explanation/Reference:

For this scenario, the best way to achieve the required solution is to use a combination of Tags and IAM policies. You can define the tags on the UAT and production EC2 instances and add a condition to the IAM policy which allows access to specific tags.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it.



By default, IAM users don't have permission to create or modify Amazon EC2 resources, or perform tasks using the Amazon EC2 API. (This means that they also can't do so using the Amazon EC2 console or CLI.) To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant IAM users permission to use the specific resources and API actions they'll need, and then attach those policies to the IAM users or groups that require those permissions.

Hence, the correct answer is: Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.

The option that says: Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering is incorrect because these are just network changes to your cloud architecture and don't have any effect on the security permissions of your users to access your EC2 instances.

The option that says: Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that are used for production or development is incorrect because the AWS Resource Access Manager (RAM) is primarily used to securely share your resources across AWS accounts or within your Organization and not on a single AWS account. You also have to set up a custom IAM Policy in order for this to work.

The option that says: Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication is incorrect because placing the EC2 instances to different AZs will only improve the availability of the systems but won't have any significance in terms of security. You have to set up an IAM Policy that allows access to EC2 instances based on their tags. In addition, a Multi-Factor Authentication is not a suitable security feature to be implemented for this scenario.

References:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-for-amazon-ec2.html>

Check out this Amazon EC2 Cheat Sheet:

QUESTION 32

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 is set to short polling so some messages are not being picked up
- D. The web application does not have permission to consume messages in the SQS queue.

Correct Answer: A

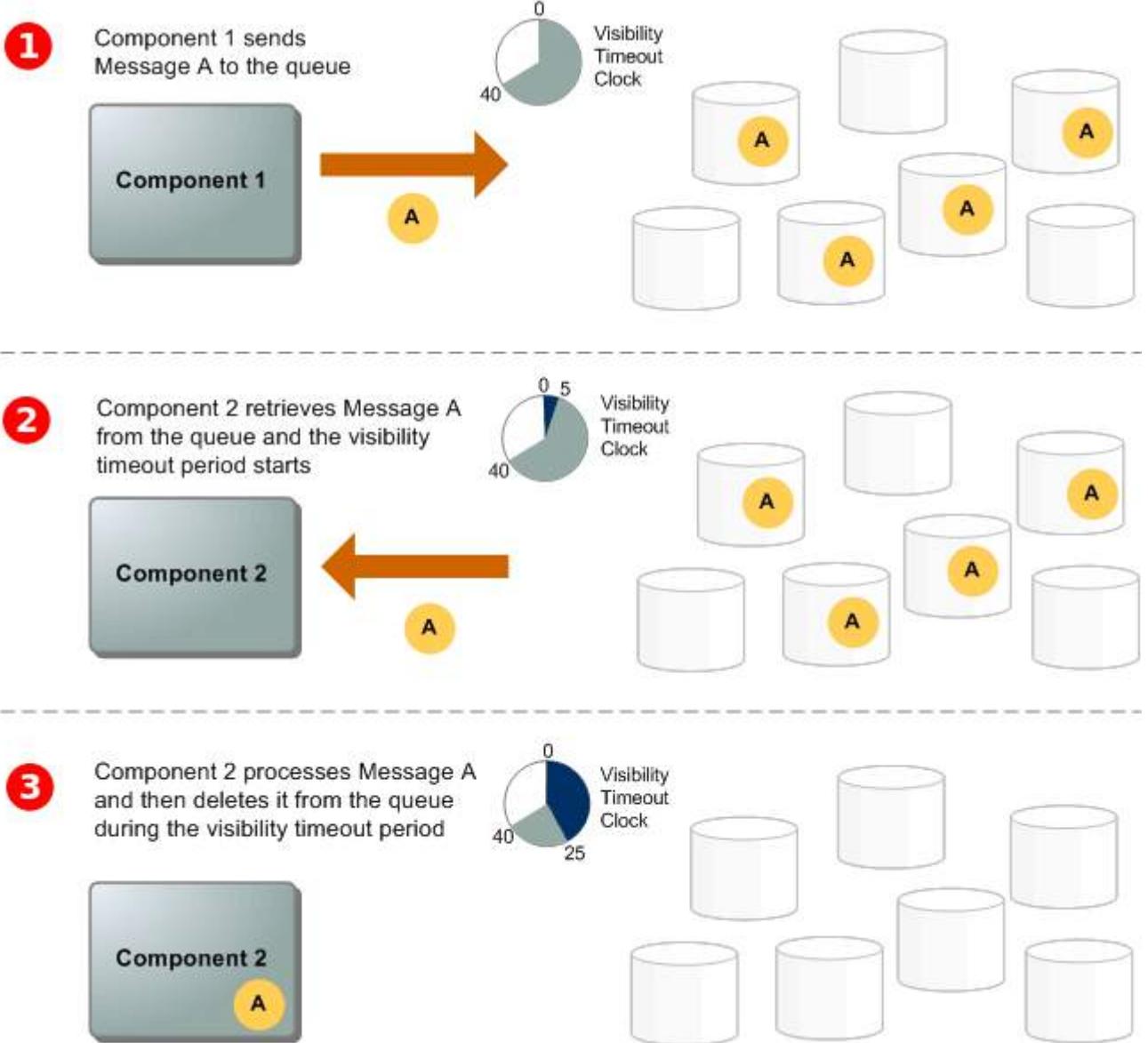
Explanation/Reference:

Always remember that the messages in the SQS queue will continue to exist even after the EC2 instance has processed it, until you delete that message. You have to ensure that you delete the message after processing to prevent the message from being received and processed again once the visibility timeout expires.

There are three main parts in a distributed messaging system:

1. The components of your distributed system (EC2 instances)
2. Your queue (distributed on Amazon SQS servers)
3. Messages in the queue.

You can set up a system which has several components that send messages to the queue and receive messages from the queue. The queue redundantly stores the messages across multiple Amazon SQS servers.



Refer to the third step of the SQS Message Lifecycle:

Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly.

When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned. While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout.

Component 2 deletes Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

The option that says: The web application is set for long polling so the messages are being sent twice is incorrect because long polling helps reduce the cost of using SQS by eliminating the number of empty responses (when there are no messages available for a ReceiveMessage request) and false empty responses (when messages are available but aren't included in a response). Messages being sent twice in an SQS queue configured with long polling is quite unlikely.

The option that says: The web application is set to short polling so some messages are not being picked up is incorrect since you are receiving emails from SNS where messages are certainly being processed. Following the scenario, messages not being picked up won't result into 20 messages being sent to your inbox.

The option that says: The web application does not have permission to consume messages in the SQS queue is incorrect because not having the correct permissions would have resulted in a different response. The scenario says that messages were properly processed but there were over 20 messages that were sent, hence, there is no problem with the accessing the queue.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html>

Check out this Amazon SQS Cheat Sheet:

<https://tutorialsdojo.com/amazon-sqs/>

QUESTION 33

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security. Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Configure Amazon CloudFront in front of the website to use HTTPS functionality
- B. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality
- C. Create and deploy an AWS Lambda function to manage and serve the website content.
- D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
- E. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer

Correct Answer: A,D

QUESTION 34

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

Correct Answer: D

Explanation/Reference:

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. Amazon FSx for Windows File Server has the features, performance, and compatibility to easily lift and shift enterprise applications to the AWS Cloud. It is accessible from Windows, Linux, and macOS compute instances and devices. Thousands of compute instances and devices can access a file system concurrently.



In this scenario, you need to migrate your existing file share configuration to the cloud. Among the options given, the best possible answer is Amazon FSx. A file share is a specific folder in your file system, including the folder's subfolders, which you make accessible to your compute instances via the SMB protocol. To migrate file share configurations from your on-premises file system, you must migrate your files first to Amazon FSx before migrating your file share configuration.

Hence, the correct answer is: Migrate the existing file share configuration to Amazon FSx for Windows File Server.

The option that says: Migrate the existing file share configuration to AWS Storage Gateway is incorrect because AWS Storage Gateway is primarily used to integrate your on-premises network to AWS but not for migrating your applications. Using a file share in Storage Gateway implies that you will still keep your on-premises systems, and not entirely migrate it.

The option that says: Migrate the existing file share configuration to Amazon EFS is incorrect because it is stated in the scenario that the company is using a file share that runs on a Windows server.

Remember that Amazon EFS only supports Linux workloads.

The option that says: Migrate the existing file share configuration to Amazon EBS is incorrect because EBS is primarily used as block storage for EC2 instances and not as a shared file system. A file share is a specific folder in a file system that you can access using a server message block (SMB) protocol. Amazon EBS does not support SMB protocol.

References:

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-file-share-config-to-fsx.html>

Check out this Amazon FSx Cheat Sheet:

<https://tutorialsdojo.com/amazon-fsx/>

QUESTION 35

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 instances are using the wrong AMI.
- B. The wrong instance type was used for the EC2 instance.
- C. The wrong subnet was used in your VPC
- D. The health check configuration is not properly defined.

Correct Answer: D

Explanation/Reference:

Since the security group is properly configured, the issue may be caused by a wrong health check configuration in the Target Group.

Edit health check X

Protocol i

Path i

Advanced health check settings

Port i	<input checked="" type="radio"/> traffic port <input type="radio"/> override
Healthy threshold i	<input type="text" value="2"/>
Unhealthy threshold i	<input type="text" value="2"/>
Timeout i	<input type="text" value="6"/> seconds
Interval i	<input type="text" value="30"/> seconds
Success codes i	<input type="text" value="200-399"/>

Cancel Save

Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

AWS Elastic Load Balancing Overview:

<https://www.youtube.com/watch?v=UBI5dw59DO8>

Check out this AWS Elastic Load Balancing (ELB) Cheat Sheet:

<https://tutorialsdojo.com/aws-elastic-load-balancing-elb/>

ELB Health Checks vs Route 53 Health Checks For Target Health Monitoring:

<https://tutorialsdojo.com/elb-health-checks-vs-route-53-health-checks-for-target-health-monitoring/>

QUESTION 36

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.

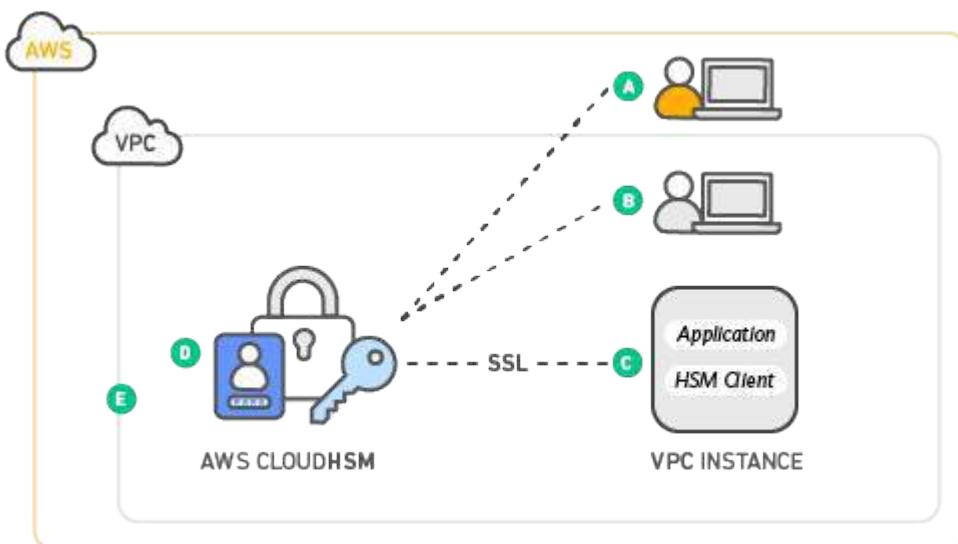
How can you obtain a new copy of the keys that you have stored on Hardware Security Module?

- A. Restore a snapshot of the Hardware Security Module.
- B. Use the Amazon CLI to get a copy of the keys.
- C. The keys are lost permanently if you did not have a copy.
- D. Contact AWS Support and they will provide you a copy of the keys.

Correct Answer: C

Explanation/Reference:

Attempting to log in as the administrator more than twice with the wrong password zeroizes your HSM appliance. When an HSM is zeroized, all keys, certificates, and other data on the HSM is destroyed. You can use your cluster's security group to prevent an unauthenticated user from zeroizing your HSM.



Amazon does not have access to your keys nor to the credentials of your Hardware Security Module (HSM) and therefore has no way to recover your keys if you lose your credentials. Amazon strongly recommends that you use two or more HSMs in separate Availability Zones in any production CloudHSM Cluster to avoid loss of cryptographic keys.

Refer to the CloudHSM FAQs for reference:

Q: Could I lose my keys if a single HSM instance fails?

Yes. It is possible to lose keys that were created since the most recent daily backup if the CloudHSM cluster that you are using fails and you are not using two or more HSMs. Amazon strongly recommends that you use two or more HSMs, in separate Availability Zones, in any production CloudHSM Cluster to avoid loss of cryptographic keys.

Q: Can Amazon recover my keys if I lose my credentials to my HSM?

No. Amazon does not have access to your keys or credentials and therefore has no way to recover your keys if you lose your credentials.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/stop-cloudhsm/>

<https://aws.amazon.com/cloudhsm/faqs/>

<https://d1.awsstatic.com/whitepapers/Security/security-of-aws-cloudhsm-backups.pdf>

QUESTION 37

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.

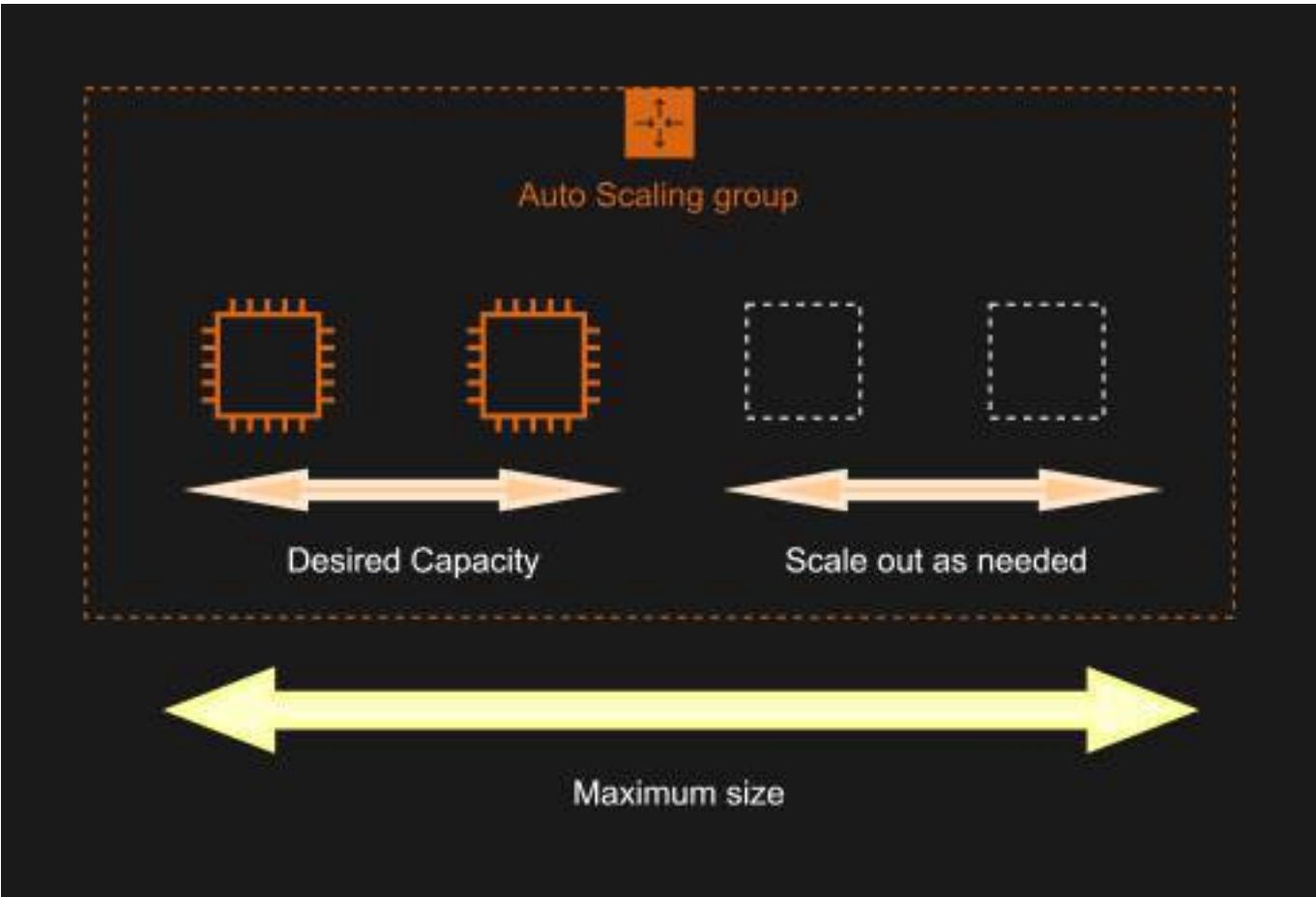
Which of the following can be done to ensure that the application works properly at the beginning of the day?

- A. Configure a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization.
- 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 Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day.

Correct Answer: D

Explanation/Reference:

Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.



To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

Hence, configuring a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day is the correct answer. You need to configure a Scheduled scaling policy. This will ensure that the instances are already scaled up and ready before the start of the day since this is when the application is used the most.

Configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization and configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization are both incorrect because although these are valid solutions, it is still better to configure a Scheduled scaling policy as you already know the exact peak hours of your application. By the time either the CPU or Memory hits a peak, the application already has performance issues, so you need to ensure the scaling is done beforehand using a Scheduled scaling policy.

Setting up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances is incorrect. Although the Application load balancer can also balance the traffic, it cannot increase the instances based on demand.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Check out this AWS Auto Scaling Cheat Sheet:

<https://tutorialsdojo.com/aws-auto-scaling/>

QUESTION 38

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive. Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: B

QUESTION 39

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:

TutorialsDojo	sg-a282cf6	launch-wizard-3	vpc-f2bf5897	
Security Group: sg-a282cf6				
Description	Inbound	Outbound	Tags	
Edit				
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	igw-b51618cc	Active	No

Which of the below steps would resolve the issue?

- A. In the Security Group, add an Inbound HTTP rule.
- B. In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc
- C. In the Security Group, remove the SSH rule.
- D. In the Route table, add this new route entry: 10.0.0.0/27 -> local

Correct Answer: A

Explanation/Reference:

In this particular scenario, you can already connect to the EC2 instance via SSH. This means that there is no problem in the Route Table of your VPC. To fix this issue, you simply need to update your Security Group and add an Inbound rule to allow HTTP traffic.

Create Security Group

Security group name: Web Server Security Group

Description: Security for production web server.

VPC: vpc-e68d9c81 | DefaultVPC (default)

Security group rules:

Inbound Outbound

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	Admin access
HTTP	TCP	80	Anywhere	Web traffic
HTTPS	TCP	443	Custom	Secure web traffic

Add Rule

Cancel Create

The option that says: In the Security Group, remove the SSH rule is incorrect as doing so will not solve the issue. It will just disable SSH traffic that is already available.

The options that say: In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc and In the Route table, add this new route entry: 10.0.0.0/27 -> local are incorrect as there is no need to change the Route Tables.

Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html
Check out this Amazon VPC Cheat Sheet:
<https://tutorialsdojo.com/amazon-vpc/>

QUESTION 40

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 Server-Side Encryption (SSE) with EC2 key pair.
- B. Set up Client-Side Encryption with Amazon S3 managed encryption keys.
- C. Set up Server-Side Encryption with keys stored in a separate S3 bucket.
- D. Set up Client-Side Encryption with a customer master key stored in AWS Key Management Service (AWS KMS).
- E. Set up Client-Side Encryption using a client-side master key.

Correct Answer: D,E

Explanation/Reference:

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3:

Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

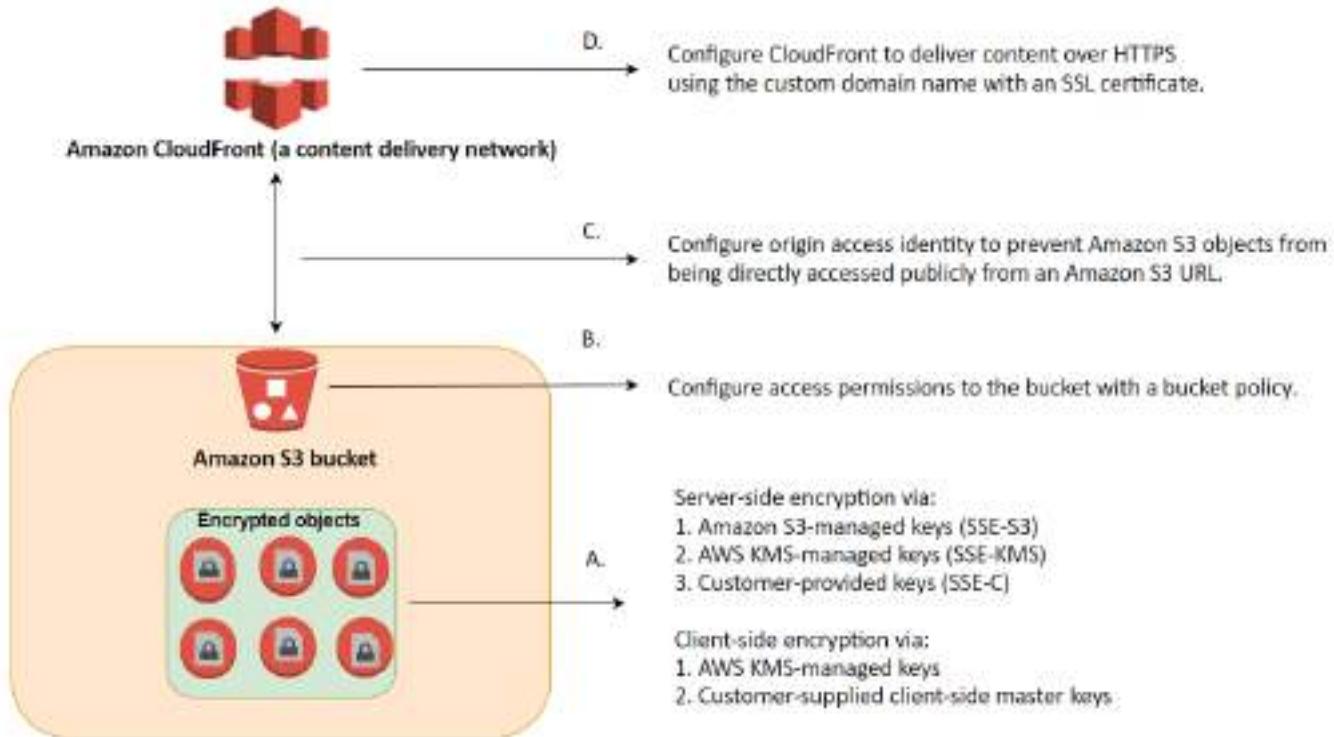
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS-Managed Customer Master Key (CMK)

Use Client-Side Encryption Using a Client-Side Master Key



Hence, the correct answers are:

- Set up Client-Side Encryption with a customer master key stored in AWS Key Management Service (AWS KMS).
- Set up Client-Side Encryption using a client-side master key.

The option that says: Set up Server-Side Encryption with keys stored in a separate S3 bucket is incorrect because you have to use AWS KMS to store your encryption keys or alternatively, choose an AWS-managed CMK instead to properly implement Server-Side Encryption in Amazon S3. In addition, storing any type of encryption key in Amazon S3 is actually a security risk and is not recommended. The option that says: Set up Client-Side encryption with Amazon S3 managed encryption keys is incorrect because you can't have an Amazon S3 managed encryption key for client-side encryption. As its name implies, an Amazon S3 managed key is fully managed by AWS and also rotates the key automatically without any manual intervention. For this scenario, you have to set up a customer

master key (CMK) in AWS KMS that you can manage, rotate, and audit or alternatively, use a client-side master key that you manually maintain.

The option that says: Set up Server-Side encryption (SSE) with EC2 key pair is incorrect because you can't use a key pair of your Amazon EC2 instance for encrypting your S3 bucket. You have to use a client-side master key or a customer master key stored in AWS KMS.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

Check out this Amazon S3 Cheat Sheet:

<https://tutorialsdojo.com/amazon-s3/>

QUESTION 41

An application is loading hundreds of JSON documents into an Amazon S3 bucket every hour which is registered in AWS Lake Formation as a data catalog. The Data Analytics team uses Amazon Athena to run analyses on these data, but due to the volume, most queries take a long time to complete. What change should be made to improve the query performance while ensuring data security?

- A. Convert the JSON documents into CSV format. Provide fine-grained named resource access control to specific databases or tables in AWS Lake Formation.
- B. Transform the JSON data into Apache Parquet format. Ensure that the user has an `lakeformation:GetDataAccess` IAM permission for underlying data access control.
- C. Compress the data into GZIP format before storing it in the S3 bucket. Apply an IAM policy with `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Lake Formation that prevents cross-service confused deputy problems and other security issues.
- D. Apply minification on the data and implement the Lake Formation tag-based access control (LF-TBAC) authorization strategy to ensure security.

Correct Answer: B

Explanation/Reference:

Amazon Athena supports a wide variety of data formats like CSV, TSV, JSON, or Textfiles and also supports open-source columnar formats such as Apache ORC and Apache Parquet. Athena also supports compressed data in Snappy, Zlib, LZO, and GZIP formats. By compressing, partitioning, and using columnar formats you can improve performance and reduce your costs.

Parquet and ORC file formats both support predicate pushdown (also called predicate filtering).

Parquet and ORC both have blocks of data that represent column values. Each block holds statistics for the block, such as max/min values. When a query is being executed, these statistics determine whether the block should be read or skipped.

Athena charges you by the amount of data scanned per query. You can save on costs and get better performance if you partition the data, compress data, or convert it to columnar formats such as Apache Parquet.

Dataset	Size on Amazon S3	Query Run time	Data Scanned	Cost
Data stored as CSV files	1 TB	236 seconds	1.15 TB	\$5.75
Data stored in Apache Parquet format*	130 GB	6.78 seconds	2.51 GB	\$0.01
Savings / Speedup	87% less with Parquet	34x faster	99% less data scanned	99.7% savings

Apache Parquet is an open-source columnar storage format that is 2x faster to unload and takes up 6x less storage in Amazon S3 as compared to other text formats. One can COPY Apache Parquet and Apache ORC file formats from Amazon S3 to your Amazon Redshift cluster. Using AWS Glue, one can configure and run a job to transform CSV data to Parquet. Parquet is a columnar format that is well suited for AWS analytics services like Amazon Athena and Amazon Redshift Spectrum.

When an integrated AWS service requests access to data in an Amazon S3 location that is access-controlled by AWS Lake Formation, Lake Formation supplies temporary credentials to access the data. To enable Lake Formation to control access to underlying data at an Amazon S3 location, you register that location with Lake Formation.

To enable Lake Formation principals to read and write underlying data with access controlled by Lake Formation permissions:

- The Amazon S3 locations that contain the data must be registered with Lake Formation.
- Principals who create Data Catalog tables that point to underlying data locations must have data location permissions.
- Principals who read and write underlying data must have Lake Formation data access permissions on the Data Catalog tables that point to the underlying data locations.
- Principals who read and write underlying data must have the lakeformation:GetDataAccess IAM permission.

Thus, the correct answer is: Transform the JSON data into Apache Parquet format. Ensure that the user has an lakeformation:GetDataAccess IAM permission for underlying data access control.

The option that says: Convert the JSON documents into CSV format. Provide fine-grained named resource access control to specific databases or tables in AWS Lake Formation is incorrect because Athena queries performed against row-based formats like CSV are slower than columnar file formats like Apache Parquet.

The option that says: Apply minification on the data and implement the Lake Formation tag-based access control (LF-TBAC) authorization strategy using IAM Tags to ensure security is incorrect.

Although minifying the JSON file might reduce its overall file size, there won't be a significant difference in terms of querying performance. LF-TBAC is a type of an attribute-based access control (ABAC) that defines permissions based on certain attributes, such as tags in AWS. LF-TBAC uses LF-Tags to grant Lake Formation permissions and not regular IAM Tags.

The option that says: Compress the data into GZIP format before storing in the S3 bucket. Apply an IAM policy with aws:SourceArn and aws:SourceAccount global condition context keys in Lake Formation that prevents cross-service confused deputy problems and other security issues. is incorrect. Compressing the files prior to storing them in Amazon S3 will only save storage costs. As for query performance, it won't have much improvement. In addition, using an IAM Policy to prevent cross-service confused deputy issues is not warranted in this scenario. Having an lakeformation:GetDataAccess IAM permission for underlying data access control should suffice.

References:

<https://aws.amazon.com/blogs/big-data/top-10-performance-tuning-tips-for-amazon-athena/>

<https://docs.aws.amazon.com/lake-formation/latest/dg/access-control-underlying-data.html>

<https://docs.aws.amazon.com/lake-formation/latest/dg/TBAC-overview.html>

Check out this Amazon Athena Cheat Sheet:

<https://tutorialsdojo.com/amazon-athena/>

QUESTION 42

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. Amazon SNS
- B. Amazon SQS
- C. AWS CloudFormation
- D. AWS Elastic Beanstalk

Correct Answer: C

Explanation/Reference:

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS.



The screenshot shows the AWS CloudFormation console's template editor. The editor displays a JSON template with several resources defined. At the top right, there is a "Choose template language" dropdown set to "JSON". The template includes resources for a VPC, Subnets, and a Route Table.

```
template1
1+ {
2+   "AWSTemplateFormatVersion": "2010-09-09",
3+   "Description": "AWS CloudFormation Sample Template VPC_AutoScaling_and_ElasticLoadBalancer: Create a load balanced, auto-scaled sample website.",
4+   "Parameters": {
5+     "VpcId": {
6+       "Type": "AWS::EC2::VPC::Id",
7+       "Description": "VpcId of your existing Virtual Private Cloud (VPC).",
8+       "ConstraintDescription": "Must be the VPC Id of an existing Virtual Private Cloud."
9+     },
10+    "Subnets": {
11+      "Type": "List[AWS::EC2::Subnet::Id]",
12+      "Description": "The list of Subnets in your Virtual Private Cloud (VPC).",
13+      "ConstraintDescription": "Must be a List of existing subnets in the selected Virtual Private Cloud."
14+    },
15+    "Asg": {
16+      "Type": "List[CloudFormation::Interface::Value]"
17+    }
18+  }
19+ }
```

You can create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. With this, you can deploy an exact copy of your AWS architecture, along with all of the AWS resources which are hosted in one region to another. Hence, the correct answer is AWS CloudFormation.

AWS Elastic Beanstalk is incorrect. Elastic Beanstalk is a high-level service that simplifies the creation of application resources such as an EC2 instance with preconfigured proxy servers (Nginx or Apache), a load balancer, an auto-scaling group, and so on. Elastic Beanstalk environments have limited resources; for example, Elastic Beanstalk does not create a VPC for you. CloudFormation on the other hand is more of a low-level service that you can use to model the entirety of your AWS environment. In fact, Elastic Beanstalk uses CloudFormation under the hood to create resources.

Amazon SQS and Amazon SNS are both incorrect because SNS and SQS are just messaging services.

References:

[<https://www.dumpscollege.com/exam/SAA-C03>](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-cli-creating-stack.html>

Check out this AWS CloudFormation Cheat Sheet:

<https://tutorialsdojo.com/aws-cloudformation/>

AWS CloudFormation - Templates, Stacks, Change Sets:

<https://youtu.be/9Xpuprxg7aY>

AWS Certified Solutions Architect Associate (SAA-C02)

Practice Questions 2020 (500+)



Guaranteed success, with 520 latest questions that are closest to actual exam, with detailed explanations

by TechRad.io



Over 500 questions with detailed explanations that help build knowledge and concepts which guarantees passing the actual exam.

AWS Certified Solutions Architect Associate (SAA-C02)

Practice Questions 2020 (500+)



Guaranteed success, with 520 latest questions that are closest to actual exam, with detailed explanations

by TechRad.io



Over 500 questions with detailed explanations that help build knowledge and concepts which guarantees passing the actual exam.

Instructions to use this book:

The Questions and their answers have been separated in different sections to ensure you don't accidentally peek at the answers. To check the answers, a convenient link has been placed at the end of the question which will take you to the Answer and the explanation.

To come back to the Question you were reading, two links have been placed, one before the explanation & the other after the explanation.

There are handy references embedded as hyperlinks that will directly open the webpage on your Kindle, mobile, or computer.

While we've made our best efforts to ensure the information is correct in this book, if you find any errors, or have questions, please reach out to us at contact@techradi.io

Scroll to the next page to begin.

Disclaimer :

Although the author and publisher have made every effort to ensure that the information in this book was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Question #1

A commercial bank has designed their next generation online banking platform to use a distributed system architecture. As their Software Architect, you must 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 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.
- C. 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.
- D. 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.

[Check answer to Question #1](#)

Question #2

You are working as a Solutions Architect in a global investment bank which requires corporate IT governance and cost oversight of all their AWS resources across their 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
- B. Create separate Availability Zones for each division within the corporate IT AWS account.
- C. Create separate VPCs for each division within the corporate IT AWS account.
- D. Use AWS Consolidated Billing by creating AWS Organizations to link the divisions accounts to a parent corporate account.
- E. Enable IAM cross-account access for all corporate IT administrators in each child account.

[Check answer to Question #2](#)

Question #3

You are trying to enable Cross-Region Replication to your S3 bucket but this option is disabled.

Which of the following options is a valid reason for this?

- A. The Cross-Region Replication feature is only available for Amazon S3 - RRS.
- B. This is a premium feature which is only for AWS Enterprise accounts.
- C. In order to use the Cross-Region Replication feature in S3, you need to first enable versioning on the bucket.
- D. The Cross-Region Replication feature is only available for Amazon S3 - Infrequent Access.

[Check answer to Question #3](#)

Question #4

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 Network Load Balancer.
- B. Launch a new microservice in AWS Fargate that acts as a load balancer since using an ALB or NLB with Fargate is not possible.
- C. Create a new record in Amazon Route 53 with Weighted Routing policy to load balance the incoming traffic.
- D. Launch a new Application Load Balancer.

[Check answer to Question #4](#)

Question #5

You are instructed by your manager to create a publicly accessible EC2 instance by using an Elastic IP (EIP) address and to give him 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 terminated and it has only one associated EIP.
- B. There is no cost if the instance is running and it has only one associated EIP.
- C. There is no cost if the instance is stopped and it has only one associated EIP.
- D. There is no cost if the instance is running and it has at least two associated EIP.

[Check answer to Question #5](#)

Question #6

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 CloudHSM and KMS?

- A. AWS CloudHSM should always be used for any payment transactions.
- B. No major difference. They both do the same thing.
- C. You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.
- D. 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 CloudHSM.

[Check answer to Question #6](#)

Question #7

You are working as a Cloud Engineer in a leading technology consulting firm which is using 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 you with 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. Egress-Only Internet Gateway
- B. NAT Gateway
- C. VPC Endpoint
- D. NAT Instance

[Check answer to Question #7](#)

Question #8

You are 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, you decided to launch your EC2 instances to a new cluster placement group. The system was working fine for a couple of weeks, however, when you try to add new instances to the placement group that already has running EC2 instances, you receive an 'insufficient capacity error'.

How will you 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. Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group.
- D. Create another Placement Group and launch the new instances in the new group.

[Check answer to Question #8](#)

Question #9

As the Solutions Architect, you have built a photo-sharing site for an entertainment company. The site was hosted using 3 EC2 instances in a single availability zone with a Classic Load Balancer in front to evenly distribute the incoming load.

What should you do to enable your Classic Load Balancer to bind a user's session to a specific instance?

- A. Placement Group
- B. Sticky Sessions
- C. Security Group
- D. Availability Zone

[Check answer to Question #9](#)

Question #10

You have created a VPC with a single subnet then you launched an On-Demand EC2 instance in that subnet. You have attached 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 per below:

Destination: 10.0.0.0/27, Target: local, Status: Active, Propagated: No

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

[Check answer to Question #10](#)

Question #11

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 FSx for Lustre
- C. Amazon Elastic Block Storage (EBS)
- D. Amazon FSx for Windows File Server

[Check answer to Question #11](#)

Question #12

You have several EC2 Reserved Instances in your account that needs to be decommissioned and shut down since they are no longer required. The data is still required by the Audit team.

Which of the following steps can be taken for this scenario? (Select TWO.)

- A. You can opt to sell these EC2 instances on the AWS Reserved Instance Marketplace
- B. Convert the EC2 instance to On-Demand instances
- C. Take snapshots of the EBS volumes and terminate the EC2 instances.
- D. Convert the EC2 instances to Spot instances with a persistent Spot request type.

[Check answer to Question #12](#)

Question #13

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. Elastic File System
- B. ElastiCache
- C. Amazon S3

D. EBS Volumes

[Check answer to Question #13](#)

Question #14

You are working as a Solutions Architect for a major accounting firm, and they have a legacy general ledger accounting application that needs to be moved to AWS. However, the legacy application has a dependency on multicast networking.

On this scenario, which of the following options should you consider ensuring the legacy application works in AWS?

- A. Create a virtual overlay network running on the OS level of the instance.
- B. All of the above.
- C. Create all the subnets on another VPC and enable VPC peering.
- D. Provision Elastic Network Interfaces between the subnets.

[Check answer to Question #14](#)

Question #15

Your IT Manager asks you to create a decoupled application whose process includes dependencies on EC2 instances and servers located in your company's on-premises data center.

Which of these options are you least likely to recommend as part of that process?

- A. SQS polling from an EC2 instance using IAM user credentials
- B. An SWF workflow
- C. Establish a Direct Connect connection from your on-premises network and VPC
- D. SQS polling from an EC2 instance deployed with an IAM role

[Check answer to Question #15](#)

Question #16

You recently created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to your S3, DynamoDB, Lambda, and other AWS resources of your cloud infrastructure.

Which of the following must be done to allow the user to make API calls to your 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. Assign an IAM Policy to the user to allow it to send API calls.
- D. Create a set of Access Keys for the user and attach the necessary permissions.

[Check answer to Question #16](#)

Question #17

You have designed and built a new AWS architecture. After deploying your application to an On-demand EC2 instance, you found that there is an issue in your application when connecting to port 443. After troubleshooting the issue, you added port 443 to the security group of the instance.

How long will it take before the changes are applied to all of the resources in your VPC?

- A. It takes exactly one minute for the rules to apply to all availability zones within the AWS region.
- B. Roughly around 5-8 minutes for the security rules to propagate.
- C. Immediately.
- D. Immediately after a reboot of the EC2 instances which belong to that security group.

[Check answer to Question #17](#)

Question #18

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. Create OpsWorks recipes that will automatically launch resources containing the latest version of the code.
- B. Create CloudFormation templates that have the latest configurations and code in them.
- C. Use CodeCommit to publish your code quickly in a private repository and push them to your resources for fast updates.
- D. Use deployment groups in CodeDeploy to automate code deployments in a consistent manner.

[Check answer to Question #18](#)

Question #19

A multinational corporate and investment bank is regularly processing steady workloads of accruals, loan interests, and other critical financial calculations every night at 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 nor interrupted. The CTO has decided to move their IT infrastructure to AWS to save cost and to improve the scalability of their digital financial services.

As the Senior Solutions Architect, how can you implement a cost-effective architecture in AWS for their financial system?

- A. Use Scheduled Reserved Instances, which provide compute capacity that is always available on the specified recurring schedule.
- B. 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.
- C. Use Spot EC2 Instances launched by a persistent Spot request, which can significantly lower your Amazon EC2 costs.
- D. Use On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second.

[Check answer to Question #19](#)

Question #20

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 be optionally stored in CloudTrail or in CloudWatch Logs.
- 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 only be stored in the attached EBS volumes of the EC2 instances, which were launched by AWS Elastic Beanstalk.

[Check answer to Question #20](#)

Question #21

You have 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 your 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 your users?

- A. Multi-master DynamoDB
- B. Multi-AZ RDS
- C. ElastiCache in-memory caching
- D. ELB sticky sessions

[Check answer to Question #21](#)

Question #22

You are working as an IT Consultant for a top investment firm. Your task is to ensure smooth upgrade of their accounting system in AWS to a new version without any system outages. The Technical Manager gave an advice to implement an in-place upgrade strategy while a DevOps Engineer suggested to use Blue/Green Deployment strategy instead.

Which of the following options are not the advantages of using Blue/Green Deployment over in-place upgrade strategy? (Select TWO.)

- A. Blue/green deployment is more cost-effective than in-place upgrade.
You don't need to launch a new environment with additional AWS resources.
- B. Impaired operation or downtime is minimized because impact is limited to the window of time between green environment issue

- detection and shift of traffic back to the blue environment.
- C. Blue/green deployments provide a level of isolation between your blue and green application environments, which reduce the deployment risk. The blue environment represents the current application version serving production traffic while the green one is staged running a different or upgrade version of your application.
 - D. It can simply roll the incoming traffic back to the currently working environment, in case of system failures, any time during the deployment process.
 - E. You can use Blue/Green Deployment with CodeCommit and CodeBuild to automatically deploy the new version of your application.

[Check answer to Question #22](#)

Question #23

Your company has 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. ECS
- B. AWS Elastic Beanstalk
- C. OpsWorks
- D. AWS CodeDeploy

[Check answer to Question #23](#)

Question #24

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 must 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. HTTP 200 result code and MD5 checksum.
- B. You will receive an SMS from Amazon SNS informing you that the object is successfully stored.
- C. Amazon S3 has 99.99999999% durability hence, there is no need to confirm that data was inserted.
- D. You will receive an email from Amazon SNS informing you that the object is successfully stored.

[Check answer to Question #24](#)

Question #25

You are planning to launch an application that tracks the GPS coordinates of delivery trucks in your 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 Kinesis
- B. AWS Data Pipeline
- C. Amazon AppStream
- D. Amazon Simple Queue Service

[Check answer to Question #25](#)

Question #26

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 Lambda function contains a recursive code and has been running for over 15 minutes.
- B. The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.
- 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.

[Check answer to Question #26](#)

Question #27

You are working for a startup that builds Internet of Things (IOT) devices and monitoring applications. They are using IOT sensors to monitor all data by using Amazon Kinesis configured with default settings. You then send the data to an Amazon S3 bucket after 2 days. When you checked the data in S3, only data for the last day is present and no data is present for the first day.

What is the root cause of this issue?

- A. The access of the Kinesis stream to the S3 bucket is insufficient.
- B. By default, data records in Kinesis are only accessible for 24 hours from the time they are added to a stream.
- C. Amazon S3 bucket has encountered a data loss.
- D. Someone has manually deleted the record in Amazon S3.

[Check answer to Question #27](#)

Question #28

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. Use AWS Organizations and Service Control Policies to control services on each account.
- B. Set up a common IAM policy that can be applied across all AWS accounts.
- C. 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.
- D. 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.

[Check answer to Question #28](#)

Question #29

You are building a microservices architecture in which a 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 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.
- C. 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.
- D. 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.

[Check answer to Question #29](#)

Question #30

A global medical research company has a molecular imaging system which provides each client with frequently updated images of what is happening inside the human body at the molecular and cellular level. The system is hosted in AWS and the images are hosted in an S3 bucket behind a CloudFront web distribution. There was a new batch of updated images that were uploaded in S3, however, the users were reporting that they were still seeing the old content. You need to control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

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

- A. Add Cache-Control no-cache, no-store, or private directives in the S3 bucket

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

[Check answer to Question #30](#)

Question #31

You 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. Create a role in IAM. Afterwards, assign this role to a new EC2 instance.
- B. Store your API credentials in Amazon Glacier.
- C. Encrypt the API credentials and store in any directory of the EC2 instance.
- D. Store the API credentials in the root web application directory of the EC2 instance.

[Check answer to Question #31](#)

Question #32

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 removing the Elastic Load Balancer
- B. Consider using Spot instances instead of reserved EC2 instances
- C. Consider using On-demand instances instead of Reserved EC2 instances
- D. Consider not using a Multi-AZ RDS deployment for the development and test database

[Check answer to Question #32](#)

Question #33

You are a Solutions Architect in an intelligence agency that 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 consistently lower inter-instance latency
- B. When you need high latency networking
- C. When you need a dedicated connection to your on-premises data center
- D. When you need a low packet-per-second performance
- E. When you need a higher packet per second (PPS) performance

[Check answer to Question #33](#)

Question #34

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 security group of the database tier to allow database traffic from the security group of the application servers.
- 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 Network ACL of the database subnet to deny all inbound non-database traffic from the subnet of the application-tier.
- D. Set up the Network ACL of the database subnet to allow inbound database traffic from the subnet of the application-tier.

[Check answer to Question #34](#)

Question #35

You are a Solutions Architect working for a software development company. You are planning to launch a fleet of EBS-backed EC2 instances and want to automatically assign each instance with a static private IP address which does not change even if the instances are restarted.

What should you do to accomplish this?

- A. Launch the instances in the Amazon Virtual Private Cloud (VPC).
- B. Launch the instances to multiple Availability Zones.
- C. Launch the instances to a single Availability Zone.
- D. Launch the instances in a Placement Group.
- E. Launch the instances in EC2-Classic.

[Check answer to Question #35](#)

Question #36

You are working as a Senior Solutions Architect for a data analytics company which has a VPC for their human resource department, and another VPC located on a different region for their finance department. You need to configure your 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 you set up to satisfy the above requirement?

- A. AWS Cloud Map
- B. Inter-Region VPC Peering
- C. VPN Connection
- D. VPC Endpoint

[Check answer to Question #36](#)

Question #37

You were hired as an IT Consultant in a startup cryptocurrency company that wants to go global with their international money transfer app. Your project is to make sure that the database of the app is highly available on multiple regions.

What are the benefits of adding Multi-AZ deployments in Amazon RDS? (Select TWO.)

- A. Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.
- B. Significantly increases the database performance.
- C. Provides SQL optimization.
- D. Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region.
- E. Provides enhanced database durability in the event of a DB instance component failure or an Availability Zone outage.

[Check answer to Question #37](#)

Question #38

A company needs to launch a new MySQL RDS database for its new data analytics application. The Solutions Architect needs to ensure that the database-tier must be able to quickly recover from any system crashes.

Which of the below is NOT a recommended practice for RDS?

- A. Use MyISAM as the storage engine for MySQL.
- B. Use InnoDB as the storage engine for MySQL.
- C. Partition your large tables so that file sizes does not exceed the 16 TB limit.
- D. Ensure that automated backups are enabled for the RDS

[Check answer to Question #38](#)

Question #39

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 host conditions to define rules that forward requests to different target groups based on the host name in the host header. This enables you to support multiple domains using a single load balancer.
- B. Use path conditions to define rules that forward requests to different target groups based on the URL in the request.

- C. Replace your ALB with a Classic Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request.
- 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.

[Check answer to Question #39](#)

Question #40

You are the Solutions Architect of a software development company where you are required to connect the on-premises infrastructure to their AWS cloud.

Which of the following AWS services can you use to accomplish this?
(Select TWO.)

- A. NAT Gateway
- B. VPC Peering
- C. AWS Direct Connect
- D. Amazon Connect
- E. IPsec VPN connection

[Check answer to Question #40](#)

Question #41

A startup company wants to launch a fleet of EC2 instances on AWS. Your manager wants to ensure that the Java programming language is installed automatically when the instance is launched.

In which of the below configurations can you achieve this requirement?

- A. IAM roles
- B. AWS Config
- C. EC2Config service

D. User data

[Check answer to Question #41](#)

Question #42

You are setting up the required compute resources in your VPC for your 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. General Purpose Instances
- C. Memory Optimized Instances
- D. Storage Optimized Instances

[Check answer to Question #42](#)

Question #43

You are working for a global news network where you have set up a CloudFront distribution for your web application. However, you noticed that your 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. You did not add an SSL certificate.
- B. The Cache-Control max-age directive is set to zero.
- C. 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.
- D. The file sizes of the cached objects are too large for CloudFront to handle.

[Check answer to Question #43](#)

Question #44

You are working as the Solutions Architect for a global technology consultancy firm which 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). Your manager instructed you to set up a latency-based routing to route incoming traffic for www.techrad.io to all the EC2 instances across all AWS regions.

Which of the following options can satisfy the given requirement?

- A. Use Route 53 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 a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions.

[Check answer to Question #44](#)

Question #45

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. AWS Identity and Access Management roles
- B. Web Identity Federation
- C. SAML-based Identity Federation
- D. Cross-Account Access

[Check answer to Question #45](#)

Question #46

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. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.
- B. Enable the in-transit encryption for Redis replication groups.
- C. None of the above.
- D. Do nothing. This feature is already enabled by default.
- E. Create a new Redis replication group and set the AtRestEncryptionEnabled parameter to true.

[Check answer to Question #46](#)

Question #47

You are working as a Solutions Architect in a well-funded financial startup. The CTO instructed you to launch a cryptocurrency mining server on a Reserved EC2 instance in us-east-1 region's private subnet which is using IPv6. Due to the financial data that the server contains, the system should be secured to avoid 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. NAT instances
- B. NAT Gateway

- C. Internet Gateway
- D. Egress-only Internet gateway

[Check answer to Question #47](#)

Question #48

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.

```
{ "AWSTemplateFormatVersion":"2010-09-09", "Parameters":{ "VPCId":{ "Type":"String", "Description":"techradio" }, "SubnetId":{ "Type":"String", "Description":"subnet-b46032ec" } }, "Outputs":{ "InstanceId":{ "Value":{ "Ref":"TechradioInstance" }, "Description":"Instance Id" } } }
```

Which of the following is the reason why this CloudFormation template will fail to deploy the stack?

- 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.

[Check answer to Question #48](#)

Question #49

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. Deploy Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing.
- B. Enable Hash Joins to improve the database query performance.
- C. Use an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes.
- D. Create Amazon Aurora Replicas.

[Check answer to Question #49](#)

Question #50

AWS hosts a variety of public datasets such as satellite imagery, geospatial, or genomic data that you want to use for your web application hosted in Amazon EC2. If you use these datasets, how much will it cost you?

- A. A one-time charge of \$10.
- B. No charge.
- C. \$10 per month for all datasets.
- D. \$10 per month for each dataset.

[Check answer to Question #50](#)

Question #51

You are working as a Solution Architect for a startup in Silicon Valley. Their application architecture is currently set up to store 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 you do to make the current architecture more secure?

- A. Put the access keys in Amazon Glacier instead.

- B. Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image.
- C. Put the access keys in an Amazon S3 bucket instead.
- D. 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.

[Check answer to Question #51](#)

Question #52

A company would like to archive their old yet confidential corporate files that are infrequently accessed.

Which is the MOST cost-efficient solution in AWS that you should recommend?

- A. Amazon Storage Gateway
- B. Amazon S3
- C. Amazon EBS
- D. Amazon Glacier

[Check answer to Question #52](#)

Question #53

You are working for a startup which develops an AI-based traffic monitoring service. You need to register a new domain called www.techradio-ai.com and set up other DNS entries for the other components of your system in AWS.

Which of the following is not supported by Amazon Route 53?

- A. SRV (service locator)
- B. SPF (sender policy framework)
- C. DNSSEC (Domain Name System Security Extensions)
- D. PTR (pointer record)

[Check answer to Question #53](#)

Question #54

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. Amazon EC2, Amazon DynamoDB, and Amazon S3
- D. Elastic Load Balancing, Amazon RDS with Multi-AZ, and Amazon S3

[Check answer to Question #54](#)

Question #55

You are working for a computer animation film studio that 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 your application?

- A. Use Amazon S3 Multipart Upload API.
- B. Leverage on Amazon CloudFront and use HTTP POST method to reduce latency.
- 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.

[Check answer to Question #55](#)

Question #56

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. Set up a micro-service architecture with ECS, ECR, and Fargate.
- B. 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.
- C. Use AWS Lambda and Amazon API Gateway.
- D. Host the APIs in a static S3 web hosting bucket behind a CloudFront web distribution.

[Check answer to Question #56](#)

Question #57

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 Notification Service
- B. Amazon Simple Queue Service
- C. Route 53

- D. SWF
- E. CloudWatch

[Check answer to Question #57](#)

Question #58

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 the mysql client using the --ssl-ca parameter when connecting to the database.
- B. Configure your RDS database to enable encryption.
- C. Set up an RDS database and enable the IAM DB Authentication.
- D. Launch a new RDS database instance with the Backtrack feature enabled.

[Check answer to Question #58](#)

Question #59

You are working as an AWS Engineer in a major telecommunications company in which you are tasked to make a network monitoring system. You launched an EC2 instance to host the monitoring system and used CloudWatch to monitor, store, and access the log files of your instance.

Which of the following provides an automated way to send log data to CloudWatch Logs from your Amazon EC2 instance?

- A. CloudTrail Logs agent
- B. CloudWatch Logs agent

- C. CloudTrail
- D. VPC Flow Logs

[Check answer to Question #59](#)

Question #60

You are a Solutions Architect of a tech company. You are having an issue whenever you try to connect to your newly created EC2 instance using a Remote Desktop connection from your computer. Upon checking, you have verified that the instance has a public IP and the Internet gateway and route tables are in place.

What else should you do for you to resolve this issue?

- A. You should adjust the security group to allow traffic from port 22
- B. You should create a new instance since there might be some issue with the instance
- C. You should restart the EC2 instance since there might be some issue with the instance
- D. You should adjust the security group to allow traffic from port 3389

[Check answer to Question #60](#)

Question #61

A WordPress website hosted in an EC2 instance, which has an additional EBS volume attached, was mistakenly deployed in the us-east-1a Availability Zone due to a misconfiguration in your CloudFormation template. There is a requirement to quickly rectify the issue by moving and attaching the EBS volume to a new EC2 instance in the us-east-1b Availability Zone.

As the Solutions Architect of the company, which of the following should you do to solve this issue?

- A. First, create a snapshot of the EBS volume. Afterwards, create a volume using the snapshot in the other Availability Zone.
- B. First, create a new volume in the other Availability Zone. Next, perform a disk copy of the contents from the source volume to the new volume that you have created.
- C. Detach the EBS volume and attach it to an EC2 instance residing in another Availability Zone.
- D. Create a new EBS volume in another Availability Zone and then specify the current EBS volume as the source.

[Check answer to Question #61](#)

Question #62

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. 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.
- B. Create a new IAM user that has access to modify the ELB. Delete that user when the work is completed.
- C. Provide the user temporary access to the root account for 8 hours only. Afterwards, change the password once the activity is completed.
- D. Open the port that ELB uses in a security group and then give the user access to that security group via a policy.

[Check answer to Question #62](#)

Question #63

You are working as a Senior Solutions Architect in a digital media services startup. Your current project is about a movie streaming app where you are required to launch several EC2 instances on multiple availability zones.

Which of the following will configure your load balancer to distribute incoming requests evenly to all EC2 instances across multiple Availability Zones?

- A. An Amazon Route 53 latency routing policy
- B. An Amazon Route 53 weighted routing policy
- C. Elastic Load Balancing request routing
- D. Cross-zone load balancing

[Check answer to Question #63](#)

Question #64

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. 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.
- B. 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.
- C. Enable the IAM DB authentication in RDS using the AWS Management Console.
- D. Specify the TDE option in an RDS option group that is associated with that DB instance to enable transparent data encryption (TDE).
- E. Configure the security groups of your EC2 instances and RDS to only allow traffic to and from port 443.

[Check answer to Question #64](#)

Question #65

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. Improve the performance of the stream by decreasing the number of its shards using the MergeShard command.
- 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. Replace the data stream with Amazon Kinesis Data Firehose instead.

[Check answer to Question #65](#)

Question #66

An event sourcing application is to be implemented using a microservice architecture on AWS. Each microservice consists of an API Gateway, AWS Lambda, and Amazon DynamoDB. The application will initialize when the first microservice publishes an event to an event store, then proceeds by consuming the data in the second microservice.

As a Solutions Architect, which of the following architectures should be followed?

- A. Configure the first microservice to send data to an Amazon SQS queue, then send the event log to an Amazon S3 bucket. Modify the second microservice to fetch data from the queue.
- B. Configure the first microservice to send data to Amazon S3 bucket. Modify the second microservice to fetch data from the bucket.
- C. Configure the first microservice to send data to Amazon Kinesis Data Firehose stream, then send the event log to an Amazon S3 bucket.

- Modify the second microservice to fetch data from the Kinesis stream.
- D. Configure the first microservice to send data to Amazon SNS topic, then send the event log to an Amazon S3 bucket. Modify the second microservice to fetch data from the topic.

[Check answer to Question #66](#)

Question #67

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. AWS CloudTrail
- B. Amazon API Gateway
- C. Amazon CloudWatch
- D. AWS X-Ray

[Check answer to Question #67](#)

Question #68

You are working as a solutions architect for a large financial company. They have a web application hosted in their on-premises infrastructure which 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 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.
- B. 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.
- C. 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.
- D. 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.
- 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.

[Check answer to Question #68](#)

Question #69

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 access logs on the application load balancer.
- B. Add an Amazon CloudWatch Logs agent on the application load balancer.
- C. Enable Amazon CloudWatch metrics on the application load balancer.
- D. Enable AWS CloudTrail for their application load balancer.

[Check answer to Question #69](#)

Question #70

A website is running on an Auto Scaling group of On-Demand EC2 instances which are abruptly getting terminated from time to time. To automate the monitoring process, you started to create a simple script which uses the AWS CLI to find the root cause of this issue.

Which of the following is the most suitable command to use?

- A. aws ec2 get-console-screenshot
- B. aws ec2 describe-images
- C. aws ec2 describe-instances
- D. aws ec2 describe-volume-status

[Check answer to Question #70](#)

Question #71

You created a new CloudFormation template that creates 4 EC2 instances and are connected to one Elastic Load Balancer (ELB).

Which section of the template should you configure to get the Domain Name Server hostname of the ELB upon the creation of the AWS stack?

- A. Parameters
- B. Outputs
- C. Resources
- D. Mappings

[Check answer to Question #71](#)

Question #72

You are setting up a cost-effective architecture for a log processing application which 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 your VPC. You must 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 Provisioned IOPS SSD (io1)
- C. EBS Cold HDD (sc1)
- D. EBS General Purpose SSD (gp2)

[Check answer to Question #72](#)

Question #73

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. Enable Enhanced Networking with Elastic Fabric Adapter (EFA) on the Windows EC2 Instances.

- B. 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.
- C. Enable Enhanced Networking with Intel 82599 Virtual Function (VF) interface on the Windows EC2 Instances.
- D. Enable Enhanced Networking with Elastic Network Adapter (ENA) on the Windows EC2 Instances.

[Check answer to Question #73](#)

Question #74

You have just launched a new API Gateway service which uses AWS Lambda as a serverless computing service.

In what type of protocol will your API endpoint be exposed?

- A. HTTP
- B. HTTPS
- C. WebSocket
- D. HTTP/2

[Check answer to Question #74](#)

Question #75

You are an IT Consultant for a top investment bank which is in the process of building its 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. 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.
- C. 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.
- 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.

[Check answer to Question #75](#)

Question #76

You are working for a top IT Consultancy that has a VPC with two On-Demand EC2 instances with Elastic IP addresses. You were notified that your EC2 instances are currently under SSH brute force attacks over the Internet. Their IT Security team has identified the IP addresses where these attacks originated. You must 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 your instances?

- A. Place the EC2 instances into private subnets
- B. Block the IP addresses in the Network Access Control List
- C. Remove the Internet Gateway from the VPC
- D. Assign a static Anycast IP address to each EC2 instance

[Check answer to Question #76](#)

Question #77

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. Choose the Availability Zone with the greatest number of instances, which is the us-west-1a Availability Zone in this scenario.
- B. Select the instances with the oldest launch configuration.
- C. Select the instance that is closest to the next billing hour.
- D. Select the instance that is farthest to the next billing hour.
- 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 most recent launch configuration.

[Check answer to Question #77](#)

Question #78

You are working as a Principal Solutions Architect for a leading digital news company which has both an on-premises data center as well as an 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 are heavily used for only a week (7 days) but after that period, it will only be infrequently used by their customers. You are 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 you can implement to meet the above requirement? (Select TWO.)

- A. Set a lifecycle policy in the bucket to transition the data to Glacier after one week (7 days).
- B. Set a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days).
- C. Set a lifecycle policy in the bucket to transition the data to S3 Glacier Deep Archive storage class 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 - Standard IA storage class after one week (7 days).

[Check answer to Question #78](#)

Question #79

A Junior DevOps Engineer deployed a large EBS-backed EC2 instance to host a NodeJS web app in AWS which was developed by an IT contractor. He properly configured the security group and used a key pair named "techradiokey" which has a techradiokey.pem private key file. The EC2 instance works as expected and the junior DevOps engineer can connect to it using an SSH connection. The IT contractor was also given the key pair and he has made various changes in the instance as well to the files located in .ssh folder to make the NodeJS app work. After a few weeks, the IT contractor and the junior DevOps engineer cannot connect the EC2 instance anymore, even with a valid private key file. They are constantly getting a "Server refused our key" error even though their private key is valid.

In this scenario, which one of the following options is not a possible reason for this issue?

- A. You don't have permissions for your authorized_keys file.
- B. The SSH private key that you are using has a file permission of 0777.

- C. You're using an SSH private key but the corresponding public key is not in the authorized_keys file.
- D. You don't have permissions for the .ssh folder.

[Check answer to Question #79](#)

Question #80

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-IA.
- B. Upload the data to S3 then use a lifecycle policy to transfer data to S3 One Zone-IA.
- C. Upload the data to Amazon FSx for Windows File Server using the Server Message Block (SMB) protocol.
- D. Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.

[Check answer to Question #80](#)

Question #81

You are working as a Solutions Architect for a leading technology company where you are instructed to troubleshoot the operational issues of your cloud architecture by logging the AWS API call history of your AWS resources. You need to quickly identify the most recent changes made to resources in your 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).
- B. Use CloudTrail and configure the destination Amazon Glacier archive to use Server-Side Encryption (SSE).
- C. Use CloudTrail and configure the destination S3 bucket to use Server-Side Encryption (SSE) with AES-128 encryption algorithm.
- D. Use CloudTrail with its default settings

[Check answer to Question #81](#)

Question #82

A data analytics company keeps a massive volume of data which 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 which frequently access 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. Cached Volume Gateway
- B. Tape Gateway
- C. Stored Volume Gateway
- D. File Gateway

[Check answer to Question #82](#)

Question #83

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. Missing permissions in SQS.
- B. The SQS queue is set to short-polling.
- C. The batch job application is configured to long polling.
- D. Amazon SQS has automatically deleted the messages that have been in a queue for more than the maximum message retention period.

[Check answer to Question #83](#)

Question #84

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 instances 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. The outbound network ACL needs to be modified to allow outbound traffic.
- B. No action needed. It can already be accessed from any IP address using SSH.
- C. The outbound security group needs to be modified to allow outbound traffic.
- D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic.

[Check answer to Question #84](#)

Question #85

You are planning to migrate a MySQL database from your on-premises data center to your AWS Cloud. This database will be used by a legacy batch application which 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 which 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 Cold HDD (sc1)
- C. Amazon EBS Provisioned IOPS SSD (io1)
- D. Amazon EBS General Purpose SSD (gp2)

[Check answer to Question #85](#)

Question #86

You have 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 must add a health check configuration to ensure your application is highly-available.

Which health checks will you implement?

- A. TCP health check
- B. FTP health check
- C. HTTP or HTTPS health check
- D. ICMP health check

[Check answer to Question #86](#)

Question #87

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. Amazon Redshift
- B. Amazon S3
- C. AWS Glue
- D. Glacier Select
- E. Amazon Athena

[Check answer to Question #87](#)

Question #88

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. Restore a snapshot of the Hardware Security Module.
- B. Contact AWS Support and they will provide you a copy of the keys.
- 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.

[Check answer to Question #88](#)

Question #89

Your IT Director instructed you to ensure that all the AWS resources in your VPC dont go beyond their respective service limits. You should prepare a system that provides you real-time guidance in provisioning your 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

[Check answer to Question #89](#)

Question #90

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 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 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.

- 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. 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.
- 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.

[Check answer to Question #90](#)

Question #91

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. Heterogeneous database migration is not supported in AWS. You must transform your database first to PostgreSQL and then migrate it to RDS.
- 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. 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.
- 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.

[Check answer to Question #91](#)

Question #92

You have EC2 instances running on your VPC. You have both UAT and production EC2 instances running. You want to ensure that employees who are responsible for the UAT instances don't have the access to work on the production instances to minimize security risks.

Which of the following would be the best way to achieve this?

- A. Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication.

- B. Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.
- C. Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that are used for production or development.
- D. Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering.

[Check answer to Question #92](#)

Question #93

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. DynamoDB
- B. Amazon Neptune
- C. Amazon Aurora
- D. SimpleDB

[Check answer to Question #93](#)

Question #94

A web application is deployed in an On-Demand EC2 instance in your VPC. There is an issue with the application which requires you to connect to it via an SSH connection.

Which of the following is needed in order to access an EC2 instance from the Internet? (Select THREE.)

- A. A Public IP address attached to the EC2 instance.

- B. A Private Elastic IP address attached to the EC2 instance.
- C. A Private IP address attached to the EC2 instance.
- D. An Internet Gateway (IGW) attached to the VPC.
- E. A route entry to the Internet gateway in the Route table of the VPC.
- F. A VPN Peering connection.

[Check answer to Question #94](#)

Question #95

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 since they do not have the option to extend their on-premises storage, which is why they are looking for a durable and scalable storage service to use in AWS.

What is the best solution for this scenario?

- A. Use a fleet of EC2 instances with EBS volumes to store the commonly used data.
- B. Use the Amazon Storage Gateway - Cached Volumes.
- C. Use both ElastiCache and S3 for frequently accessed data.
- D. Use Amazon Glacier.

[Check answer to Question #95](#)

Question #96

You are working as an IT Consultant for a large media company where you are tasked to design a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. You expect this S3 bucket to immediately receive over 2000 PUT requests and 3500 GET requests per second at peak hour.

What should you do to ensure optimal performance?

- A. Add a random prefix to the key names.

- B. Use Byte-Range Fetches to retrieve multiple ranges of an object data per GET request.
- C. Do nothing. Amazon S3 will automatically manage performance at this scale.
- D. Use a predictable naming scheme in the key names such as sequential numbers or date time sequences.

[Check answer to Question #96](#)

Question #97

You are a Solutions Architect working for a startup which is currently migrating their production environment to AWS. Your manager asked you to set up access to the AWS console using Identity Access Management (IAM). Using the AWS CLI, you have created 5 users for your systems administrators.

What further steps do you need to take for your systems administrators to get access to the AWS console?

- A. Enable multi-factor authentication on their accounts and define a password policy.
- B. Add the administrators to the Security Group.
- C. Provide a password for each user created and give these passwords to your system administrators.
- D. Provide the system administrators the secret access key and access key id.

[Check answer to Question #97](#)

Question #98

You are setting up a configuration management in your existing cloud architecture where you must deploy and manage your 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 CodeDeploy
- B. AWS Elastic Beanstalk
- C. AWS CloudFormation
- D. AWS OpsWorks

[Check answer to Question #98](#)

Question #99

You are managing a global news website which has a very high traffic. To improve the performance, you redesigned the application architecture to use a Classic Load Balancer with an Auto Scaling Group in multiple Availability Zones. However, you noticed that one of the Availability Zones is not receiving any traffic.

What is the root cause of this issue?

- A. The Availability Zone is not properly added to the load balancer which is why it is not receiving any traffic.
- B. The Classic Load Balancer is down
- C. Auto Scaling should be disabled for the load balancer to route the traffic to multiple Availability Zones.
- D. By default, you are not allowed to use a load balancer with multiple Availability Zones. You must send a request form to AWS in order for this to work.

[Check answer to Question #99](#)

Question #100

You are consulted by a multimedia company that needs to deploy web services to an AWS region which they have never used before. The company currently has an IAM role for their Amazon EC2 instance which permits the instance to access Amazon DynamoDB. They want their EC2 instances in the new region to have the exact same privileges.

What should you do to accomplish this?

- A. Create an Amazon Machine Image (AMI) of the instance and copy it to the new region.
- B. In the new Region, create a new IAM role and associated policies then assign it to the new instance.
- C. Assign the existing IAM role to instances in the new region.
- D. Duplicate the IAM role and associated policies to the new region and attach it to the instances.

[Check answer to Question #100](#)

Question #101

You are working for a large financial company. In their enterprise application, they want to apply a group of database-specific settings to their Relational Database Instances.

Which of the following options can be used to easily apply the settings in one go for all the Relational database instances?

- A. NACL Groups
- B. Security Groups
- C. IAM Roles
- D. Parameter Groups

[Check answer to Question #101](#)

Question #102

A web application is hosted on an EC2 instance that processes sensitive financial information which is launched in a private subnet. All the data are stored in an Amazon S3 bucket. The 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?

- A. Change the web architecture to access the financial data in your S3 bucket through a VPN connection.

- B. Change the web architecture to access the financial data through a Gateway VPC Endpoint.
- C. Change the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink.
- D. Change the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service.

[Check answer to Question #102](#)

Question #103

You are running an 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 volume of the instance was not big enough to handle all of the processing data.
- B. The EC2 instance was using EBS backed root volumes, which are ephemeral and only live for the life of the instance.
- C. The EC2 instance was using instance store volumes, which are ephemeral and only live for the life of the instance.
- D. The instance was hit by a virus that wipes out all data.

[Check answer to Question #103](#)

Question #104

You just joined a large tech company with an existing Amazon VPC. When reviewing the Auto Scaling events, you noticed that their web application is scaling up and down multiple times within the hour.

What design change could you make to optimize cost while preserving elasticity?

- A. Add provisioned IOPS to the instances
- B. Increase the base number of Auto Scaling instances for the Auto Scaling group
- C. Increase the instance type in the launch configuration
- D. Change the cooldown period of the Auto Scaling group and set the CloudWatch metric to a higher threshold

[Check answer to Question #104](#)

Question #105

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

[Check answer to Question #105](#)

Question #106

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 an A record pointing to the IP address of the load balancer.
- C. Create a CNAME record pointing to the load balancer DNS name.
- D. Create an A record aliased to the load balancer DNS name.

[Check answer to Question #106](#)

Question #107

You are required to deploy a Docker-based batch application to your VPC 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 cost-effective option to use in implementing this architecture?

- A. Use ECS as the container management service then set up Spot EC2 Instances for processing both mission-critical and non-essential batch jobs.
- B. Use ECS as the container management service then set up Reserved EC2 Instances for processing both mission-critical and non-essential batch jobs.
- C. 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.
- D. Use ECS as the container management service then set up On-Demand EC2 Instances for processing both mission-critical and non-essential batch jobs.

[Check answer to Question #107](#)

Question #108

You are building a prototype for a cryptocurrency news website of a small startup. The website will be deployed to a Spot EC2 Linux instance and will use Amazon Aurora as its database. You requested a spot instance at a maximum price of \$0.04/hr which has been fulfilled immediately and after

90 minutes, the spot price increases to \$0.06/hr and then your instance was terminated by AWS.

In this scenario, what would be the total cost of running your spot instance?

- A. \$0.00
- B. \$0.06
- C. \$0.08
- D. \$0.07

[Check answer to Question #108](#)

Question #109

You recently launched a fleet of on-demand EC2 instances to host a massively multiplayer online role-playing game (MMORPG) server in your VPC. The EC2 instances are configured with Auto Scaling and AWS Systems Manager.

What can you use to configure your EC2 instances without having to establish an RDP or SSH connection to each instance?

- A. EC2Config
- B. Run Command
- C. AWS CodePipeline
- D. AWS Config

[Check answer to Question #109](#)

Question #110

You are working for a multinational telecommunications company. Your IT Manager is willing to consolidate their log streams including the access, application, and security logs in one single system. Once consolidated, the company wants to 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, 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.
- B. First, configure Amazon Cloud Trail to receive custom logs and then use EMR to apply heuristics on the logs.
- 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 the log events to Amazon Kinesis then afterwards, develop a client process to apply heuristics on the logs.

[Check answer to Question #110](#)

Question #111

You recently launched a news website which is expected to be visited by millions of people around the world. You chose to deploy the website in AWS to take advantage of its extensive range of cloud services and global infrastructure.

Aside from AWS Region and Availability Zones, which of the following is part of the AWS Global Infrastructure that is used for content distribution?

- A. Hypervisor
- B. Edge Location
- C. VPC Endpoint
- D. Bastion Hosts

[Check answer to Question #111](#)

Question #112

A loan processing application is hosted in a single On-Demand EC2 instance in your VPC. To improve the scalability of your application, you must 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 must 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 must ensure that the AMI used to launch the instance no longer exists.
- D. You must ensure that the AMI used to launch the instance still exists.
- E. You must ensure that the instance is in a different Availability Zone as the Auto Scaling group.

[Check answer to Question #112](#)

Question #113

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 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 a password stored in CloudHSM.
- B. By using S3 Server-Side Encryption.
- C. By using Amazon-managed keys in AWS Key Management Service (KMS).
- D. By using S3 Client-Side Encryption.
- E. By using your own keys in AWS Key Management Service (KMS).
- F. By using the SSL certificates provided by the AWS Certificate Manager (ACM).

[Check answer to Question #113](#)

Question #114

You are implementing a hybrid architecture for your company where you are connecting their Amazon Virtual Private Cloud (VPC) to their on-premises network.

Which of the following can be used to create a private connection between the VPC and your company's on-premises network?

- A. Direct Connect
- B. ClassicLink
- C. Route 53
- D. AWS Direct Link

[Check answer to Question #114](#)

Question #115

You are assigned to design a highly available architecture in AWS. You 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 the 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 instance type was used for the EC2 instance.
- B. The health check configuration is not properly defined.
- C. The wrong subnet was used in your VPC
- D. The instances are using the wrong AMI.

[Check answer to Question #115](#)

Question #116

You are designing an online banking application which needs to have a distributed session data management. Currently, the application is hosted on an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones with a Classic Load Balancer that distributes the load.

Which of the following options should you do to satisfy the given requirement?

- A. Use Amazon ElastiCache
- B. Set up an AWS Systems Manager Session Manager
- C. Enable the sticky session feature in the Classic Load Balancer
- D. Use the GetSessionToken action in AWS STS for session management

[Check answer to Question #116](#)

Question #117

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 the period during which the SQS queue prevents other consuming components from receiving and processing a message?

- A. Visibility Timeout
- B. Receiving Timeout
- C. Component Timeout
- D. Processing Timeout

[Check answer to Question #117](#)

Question #118

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. Add another rule in the AWS WAF web ACL with a geo match condition that blocks requests that originate from a specific country.
- B. 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.
- C. In the Application Load Balancer, create a listener rule that explicitly allows requests from approved IP addresses.
- 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.

[Check answer to Question #118](#)

Question #119

You are working as a Solutions Architect for a fast-growing startup which 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 on the existing security controls in AWS but can still communicate with their on-premises network.

Which set of AWS services will you use to meet these requirements?

- A. AWS Directory Services, VPN connection, and AWS Identity and Access Management
- B. AWS Directory Services, VPN connection, and Amazon Workspaces
- C. AWS Directory Services, VPN connection, and ClassicLink

D. AWS Directory Services, VPN connection, and Amazon S3

[Check answer to Question #119](#)

Question #120

You have an On-Demand EC2 instance with an attached non-root 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. On one night, there's 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 while the snapshot is in progress.
- B. The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes
- C. The EBS volume cannot be used until the snapshot completes.
- D. The EBS volume can be used in read-only mode while the snapshot is in progress.

[Check answer to Question #120](#)

Question #121

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.

[Check answer to Question #121](#)

Question #122

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. Only the data in the volume is encrypted and not all the data moving between the volume and the instance.
- B. The volumes created from the encrypted snapshot are not encrypted.
- C. Snapshots are not automatically encrypted.
- D. Snapshots are automatically encrypted.
- E. All data moving between the volume and the instance are encrypted.

[Check answer to Question #122](#)

Question #123

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. Storage Gateway
- C. S3
- D. EBS

[Check answer to Question #123](#)

Question #124

Your 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. You 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 will you 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 zero.
- C. Configure Amazon SQS to use short polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.
- D. Configure Amazon SQS to use long polling by setting the ReceiveMessageWaitTimeSeconds to a number greater than zero.

[Check answer to Question #124](#)

Question #125

You are working for a data analytics startup that collects clickstream data and stores them in an S3 bucket. You need to launch an AWS Lambda function to trigger your 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. AWS Step Functions
- B. Redshift Spectrum
- C. AWS Glue
- D. S3 Select

[Check answer to Question #125](#)

Question #126

A local bank has an in-house application which 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. Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3.
- B. Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3.
- C. Configure a VPC Gateway Endpoint along with a corresponding route entry that directs the data to S3.
- D. Configure a VPC Interface Endpoint along with a corresponding route entry that directs the data to S3.

[Check answer to Question #126](#)

Question #127

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. AWS DataSync
- C. Amazon FSx for Lustre
- D. Amazon FSx for Windows File Server

[Check answer to Question #127](#)

Question #128

Your manager instructed you to use Route 53 instead of an ELB to load balance the incoming request to your web application. The system is deployed to two EC2 instances to which the traffic needs to be distributed to.

You want to set a specific percentage of traffic to go to each instance. Which routing policy would you use?

- A. Weighted
- B. Failover
- C. Latency
- D. Geolocation

[Check answer to Question #128](#)

Question #129

An application is hosted in an Auto Scaling group of EC2 instances. To improve the monitoring process, you must 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. Target tracking scaling
- B. Scheduled Scaling
- C. Simple scaling
- D. Step scaling

[Check answer to Question #129](#)

Question #130

You are working as an IT Consultant for a large financial firm. They have a requirement to store irreproducible financial documents using Amazon S3. 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 - Infrequent Access
- B. Use Amazon S3 Standard
- C. Use Amazon Glacier Deep Archive
- D. Use Amazon S3 -Intelligent Tiering

[Check answer to Question #130](#)

Question #131

An online trading platform with thousands of clients across the globe is hosted in AWS. To reduce latency, you must 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 Global Accelerator
- B. AWS PrivateLink
- C. Amazon CloudFront
- D. AWS WAF

[Check answer to Question #131](#)

Question #132

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 ap-southeast-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. Transfer Acceleration
- B. Multipart Upload
- C. Cross-Region Replication
- D. AWS Global Accelerator

[Check answer to Question #132](#)

Question #133

You are working as a Solutions Architect for a leading financial firm where you are responsible in ensuring that their 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. Amazon GuardDuty
- B. AWS Shield
- C. AWS WAF
- D. AWS Firewall Manager

[Check answer to Question #133](#)

Question #134

You are 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 automatically saved as an EBS volume.
- C. Data is automatically deleted.
- D. Data is unavailable until the instance is restarted.

[Check answer to Question #134](#)

Question #135

You are managing a global news website which 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 Read Replicas
- B. Enable Amazon RDS Standby Replicas
- C. Enable Multi-AZ deployments
- D. Use SQS to queue up the requests

[Check answer to Question #135](#)

Question #136

You are working as a Solutions Architect for a startup in which you are tasked 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 these data are to be sent to Amazon EMR for further processing. It is crucial that none of the messages will be lost, no duplicates will be produced and that they are processed in EMR in the same order as their arrival.

Which of the following options should you implement to meet the startup's requirements?

- 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 a pipeline using AWS Data Pipeline to handle the messages.
- D. Create an Amazon Kinesis Data Stream to collect the messages.

[Check answer to Question #136](#)

Question #137

A multinational company with multiple on-premises data centers around the globe is heavily using AWS to serve its clients worldwide. The company already has hundreds of VPCs with multiple VPN connections to their data centers that span to multiple AWS Regions. As the number of its workloads running on AWS grows, the company must be able to scale its networks across multiple accounts and Amazon VPCs to keep up. A Solutions Architect is tasked to interconnect all the company's on-premises networks, VPNs, and VPCs into a single gateway, that 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. 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.
- B. 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.
- C. Set up an AWS Direct Connect Gateway to achieve inter-region VPC access to all of the AWS resources and on-premises 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.
- D. Set up an AWS Transit Gateway to implement a hub-and-spoke network topology in each region that routes all traffic through a network transit center. Route traffic between VPCs and the on-premises data centers over AWS Site-to-Site VPNs.

[Check answer to Question #137](#)

Question #138

You are a Cloud Migration Engineer in a media company which uses 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.

What should you do if the company needs to automatically transfer or archive media data from an S3 bucket to Glacier?

- A. Use Amazon SWF
- B. Use Lifecycle Policies
- C. Use a custom shell script that transfers data from the S3 bucket to Glacier
- D. Use Amazon SQS

[Check answer to Question #138](#)

Question #139

You are working as a Solutions Architect for a major supermarket store chain. They have an e-commerce application which is running in eu-east-2 region that strictly always requires six EC2 instances running. In that region, there are 3 Availability Zones (AZ) - eu-east-2a, eu-east-2b, and eu-east-2c that you can use.

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 three EC2 instances, eu-east-2b with three EC2 instances, and eu-east-2c with three EC2 instances
- B. eu-east-2a with two EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances
- C. eu-east-2a with four EC2 instances, eu-east-2b with two EC2 instances, and eu-east-2c with two EC2 instances
- D. eu-east-2a with two EC2 instances, eu-east-2b with four EC2 instances, and eu-east-2c with two EC2 instances

- E. eu-east-2a with six EC2 instances, eu-east-2b with six EC2 instances, and eu-east-2c with no EC2 instances

[Check answer to Question #139](#)

Question #140

You have a requirement to integrate the Lightweight Directory Access Protocol (LDAP) directory service of your on-premises data center to your 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. Develop an on-premises custom identity broker application and use STS to issue short-lived AWS credentials.
- B. Use IAM roles to rotate the IAM credentials whenever LDAP credentials are updated.
- C. Use an IAM policy that references the LDAP identifiers and AWS credentials.
- D. Use AWS Single Sign-On (SSO) service to enable single sign-on between AWS and your LDAP.

[Check answer to Question #140](#)

Question #141

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 regions failure. In the event of an Availability Zone outage, promote any replica to become the primary instance.

[Check answer to Question #141](#)

Question #142

You have 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. Create a new launch configuration with the new instance type and update the Auto Scaling Group.
- B. Just change the instance type to t2.2xlarge in the current launch configuration
- C. Change the instance type of each EC2 instance manually.
- D. Create another Auto Scaling Group and attach the new instance type.

[Check answer to Question #142](#)

Question #143

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

[Check answer to Question #143](#)

Question #144

A newly hired Solutions Architect is checking all 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:

- i. Type: RDP, Protocol: TCP, Port Range:3389, Source: Custom – 125.80.112.72/32
- ii. Type: MSSQL, Protocol: TCP, Port Range: 1433, Source: Anywhere – 0.0.0.0/0,::0

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 static AnyCast IP address attached to the application tier.
- C. For the MS SQL rule, change the Source to the security group ID attached to the application tier.
- D. For the MS SQL rule, change the Source to the EC2 instance IDs of the underlying instances of the Auto Scaling group.

[Check answer to Question #144](#)

Question #145

You have a prototype web application that uses one Spot EC2 instance. What will happen to the instance by default if it gets interrupted by Amazon EC2 for capacity requirements?

- A. The instance will be stopped
- B. The instance will be terminated
- C. The instance will be restarted
- D. This is not possible as only On-Demand instances can be interrupted by Amazon EC2

[Check answer to Question #145](#)

Question #146

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. VPC Flow Logs
- D. AWS X-Ray

[Check answer to Question #146](#)

Question #147

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 600 then maintain a high queue length.
- C. Set the IOPS to 800 then maintain a low queue length.
- D. Set the IOPS to 500 then maintain a low queue length.

[Check answer to Question #147](#)

Question #148

You are responsible for running a global news website hosted in a fleet of EC2 Instances. Lately, the load on the website has increased which resulted to 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 CloudFront with website as the custom origin.
- B. For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions.

- C. Use Amazon ElastiCache for the website's in-memory data store or cache.
- D. Deploy the website to all regions in different VPCs for faster processing.

[Check answer to Question #148](#)

Question #149

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. SWF
- C. AWS Batch
- D. AWS Lambda

[Check answer to Question #149](#)

Question #150

A data analytics application requires a service that can collect, process, and analyze clickstream data from various websites in real-time.

Which of the following is the most suitable service to use for the application?

- A. Amazon EMR with Compute Optimized Instances
- B. AWS Glue
- C. Kinesis
- D. Redshift Spectrum

[Check answer to Question #150](#)

Question #151

A web application is hosted in an Auto Scaling group of EC2 instances deployed across multiple Availability Zones in front of 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. A private S3 bucket with versioning enabled
- B. AWS Certificate Manager
- C. IAM certificate store
- D. CloudFront
- E. An S3 bucket configured with server-side encryption with customer-provided encryption keys (SSE-C)

[Check answer to Question #151](#)

Question #152

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 which shows who used the encryption key and by whom for security purposes.

Which of the following should the Architect implement to satisfy the requirement in the most cost-effective way? (Select TWO.)

- A. Configure Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).
- B. Configure Server-Side Encryption with Customer-Provided Keys (SSE-C).

- C. Configure Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
- D. Amazon Certificate Manager
- E. Use Amazon S3 to store the data.
- F. Use Amazon S3 Glacier Deep Archive to store the data.

[Check answer to Question #152](#)

Question #153

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 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 techradio-finance prefix in the S3 bucket will be used for post-processing 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 bucket to S3-IA using lifecycle policy.
- B. Store the files in S3 then after a month, change the storage class of the bucket to Intelligent-Tiering using lifecycle policy.
- C. Store the files in S3 then after a month, change the storage class of the techradio-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 techradio-finance prefix to S3-IA while the remaining go to Glacier using lifecycle policy.

[Check answer to Question #153](#)

Question #154

You launched an EC2 instance in your newly created VPC. You have 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 DNS resolution and DNS hostname of the VPC configuration should be enabled.
- B. Amazon Route53 is not enabled.
- C. The newly created VPC has an invalid CIDR block.
- D. The security group of the EC2 instance needs to be modified.

[Check answer to Question #154](#)

Question #155

You are a Solutions Architect for a large London-based software company. You are assigned to improve the performance and current processes of supporting the AWS resources in your VPC. Upon checking, you noticed that the Operations team does not have an automated way to monitor and resolve issues with their on-demand EC2 instances.

What can be used to automatically monitor your EC2 instances and notify the Operations team for any incidents?

- A. Amazon SWF
- B. Amazon SQS
- C. Amazon CloudWatch
- D. AWS CloudTrail

[Check answer to Question #155](#)

Question #156

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 OS-bypass 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).

[Check answer to Question #156](#)

Question #157

You are planning to reduce the amount of data that Amazon S3 transfers to your servers in order to lower your operating costs as well as to 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. RDS
- B. AWS Step Functions
- C. S3 Select
- D. Redshift Spectrum

[Check answer to Question #157](#)

Question #158

A bank portal application is hosted in an Auto Scaling group of EC2 instances behind a Classic Load Balancer (CLB). You are required to set up the architecture so that any back-end EC2 instances that you de-register should complete the in-progress requests first before the de-registration process takes effect. Conversely, if a back-end instance fails health checks, the load balancer should not send any new requests to the unhealthy instance but should allow existing requests to complete.

How will you configure your load balancer to satisfy the above requirement?

- A. Configure Proxy Protocol
- B. Configure both Cross-Zone Load Balancing and Sticky Sessions
- C. Configure Sticky Sessions
- D. Configure Connection Draining

[Check answer to Question #158](#)

Question #159

You have a web-based order processing system which is currently using a standard queue in Amazon SQS. The support team noticed that there are a lot of cases where an order was processed twice. This issue has caused a lot of trouble in your processing and made your customers very unhappy. Your IT 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. Change the message size in SQS.
- B. Use an Amazon SQS FIFO Queue instead.
- C. Alter the retention period in Amazon SQS.
- D. Alter the visibility timeout of SQS.
- E. Replace Amazon SQS and instead, use Amazon Simple Workflow service.

[Check answer to Question #159](#)

Question #160

You are a Big Data Engineer who is assigned to handle the online enrollment system database of a prestigious university, which is hosted in RDS. You are 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 a more accurate information? (Select TWO.)

- A. RDS child processes.
- B. CPU Utilization
- C. Database Connections
- D. Freeable Memory
- E. OS processes

[Check answer to Question #160](#)

Question #161

You are a Solutions Architect working for a large multinational investment bank. They have 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 2 instances in each of 3 Availability Zones behind an Application Load Balancer.
- B. Deploy an Auto Scaling group with 2 instances in each of 2 Availability Zones behind an Application Load Balancer.
- C. Deploy an Auto Scaling group with 1 instance in each of 4 Availability Zones behind an Application Load Balancer.

- D. Deploy an Auto Scaling group with 4 instances in one Availability Zone behind an Application Load Balancer.

[Check answer to Question #161](#)

Question #162

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. Use Automated snapshots of your Redshift Cluster.
- B. Do nothing because Amazon Redshift is a highly available, fully-managed data warehouse which can withstand an outage of an entire AWS region.
- C. 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.
- D. Enable Cross-Region Snapshots Copy in your Amazon Redshift Cluster.

[Check answer to Question #162](#)

Question #163

Your 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:

- a) There is an application load balancer that would distribute the incoming traffic among the servers in the application tier.
- b) 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.

- c) The database tier contains very sensitive data. It must not share the same subnet with other AWS resources and its custom route table with other instances in the environment.
- d) The environment must be highly available and scalable to handle a surge of incoming traffic over the Internet.

How many subnets should you create to meet the above requirements?

- A. 4
- B. 6
- C. 2
- D. 3

[Check answer to Question #163](#)

Question #164

You are working for a large bank that is developing a web application that receives large amounts of object data. They are using the data to generate a report for their stockbrokers to use daily. Unfortunately, a recent financial crisis has left the bank short on cash and cannot afford to purchase expensive storage hardware. They had resorted to use AWS instead.

Which is the best service to use in order to store a virtually unlimited amount of object data without any effort to scale when demand unexpectedly increases?

- A. Amazon EC2
- B. Amazon S3 Glacier
- C. Amazon S3
- D. DynamoDB
- E. Amazon Import/Export

[Check answer to Question #164](#)

Question #165

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. 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.
- B. 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.
- C. 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.
- D. Upgrade the instance type of the RDS database to a large instance.

[Check answer to Question #165](#)

Question #166

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 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.
- B. 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.
- C. 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.
- D. 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.

[Check answer to Question #166](#)

Question #167

You are managing an online platform which 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 your AWS resources should be properly captured and recorded. You used CloudTrail in your VPC to help you in the compliance, operational auditing, and risk auditing of your AWS account.

In this scenario, where does CloudTrail store all the logs that it creates?

- A. An RDS instance
- B. Amazon S3
- C. Amazon Redshift
- D. DynamoDB

[Check answer to Question #167](#)

Question #168

You are working as a Solutions Architect for a financial firm which is building an internal application that processes loans, accruals, and interest rates for their clients. They require a storage service that can handle future increases in storage capacity of up to 16 TB and can provide the lowest-latency access to their data. Their web application will be hosted in a single m5ad.24xlarge Reserved EC2 instance which will process and store data to the storage service.

Which of the following would be the most suitable storage service that you should use to meet this requirement?

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

[Check answer to Question #168](#)

Question #169

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

[Check answer to Question #169](#)

Question #170

You are the technical lead of the Cloud Infrastructure team in your company and you were consulted by a software developer regarding the required AWS resources of the web application that he is building. He 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 his web application persists, the app should be launched in an EC2 instance that has a durable, block-level storage volume attached. He 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. 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.
- C. 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.
- D. 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.
- E. Reduced Redundancy Storage volumes offer consistent and low-latency performance and are designed for I/O intensive applications such as large relational or NoSQL databases.

[Check answer to Question #170](#)

Question #171

You are working for a large global media company with multiple office locations all around the world. You are 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 Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM user.
- B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
- C. Create an S3 bucket policy that lists the CloudFront distribution ID as the principal and the target bucket as the Amazon Resource Name (ARN).
- D. Add the CloudFront account security group.

[Check answer to Question #171](#)

Question #172

You have a web application hosted in an On-Demand EC2 instance in your VPC. 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 user data information from <http://169.254.169.254/latest/user-data/>
- B. By using a CloudWatch metric.
- C. By using IAM.
- D. By using a Curl or Get Command to get the latest metadata information from <http://169.254.169.254/latest/meta-data/>

[Check answer to Question #172](#)

Question #173

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 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 are possible solutions that an Architect can implement to solve this issue? (Select TWO.)

- A. Modify the scaling policy to increase the threshold to scale up the number of instances.
- B. Enable detailed monitoring on the instances.
- C. Install CloudWatch monitoring scripts in the instances. Send custom metrics to CloudWatch which will trigger your Auto Scaling group to scale up.
- D. Install AWS SDK in the EC2 instances. Create a script that will trigger the Auto Scaling event if there is a high memory usage.
- E. Install the CloudWatch agent to the EC2 instances which will trigger your Auto Scaling group to scale up.

[Check answer to Question #173](#)

Question #174

You are working for a media company and you need to configure an Amazon S3 bucket to serve static assets for your public-facing web application.

Which methods ensure that all the objects uploaded to the S3 bucket can be read publicly all over the Internet? (Select TWO.)

- A. Grant public read access to the object when uploading it using the S3 Console.
- B. Create an IAM role to set the objects inside the S3 bucket to public read.
- C. Configure the S3 bucket policy to set all objects to public read.

- D. Do nothing. Amazon S3 objects are already public by default.
- E. Configure the ACL of the S3 bucket to set all objects to be publicly readable and writeable.

[Check answer to Question #174](#)

Question #175

You are working for a tech company which currently has an on-premises infrastructure. They are currently running low on storage and want to have the ability to extend their storage using AWS cloud.

Which AWS service can help you achieve this requirement?

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

[Check answer to Question #175](#)

Question #176

A web application always requires a minimum of six Amazon Elastic Compute Cloud (EC2) instances running. 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. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and no instances in eu-west-1c
- B. 3 instances in eu-west-1a, 3 instances in eu-west-1b, and 3 instances in eu-west-1c

- C. 2 instances in eu-west-1a, 2 instances in eu-west-1b, and 2 instances in eu-west-1c
- D. 6 instances in eu-west-1a, 6 instances in eu-west-1b, and 6 instances in eu-west-1c

[Check answer to Question #176](#)

Question #177

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. Develop a custom application that integrates with Cognito that implements a second layer of authentication.
- C. Integrate Cognito with Amazon SNS Mobile Push to allow additional authentication via SMS.
- D. Add multi-factor authentication (MFA) to a user pool in Cognito to protect the identity of your users.

[Check answer to Question #177](#)

Question #178

You recently 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 your IP address 175.45.116.100 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: UDP 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: TCP 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

[Check answer to Question #178](#)

Question #179

You are employed by a large electronics company that uses Amazon Simple Storage Service. 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 the Requester Pays option to track access via AWS Billing.
- B. Enable server access logging for all required Amazon S3 buckets.
- C. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
- D. Enable Amazon S3 Event Notifications for PUT and POST.

[Check answer to Question #179](#)

Question #180

You have a distributed application in AWS that periodically processes large volumes of data across multiple instances. You designed the application to recover gracefully from any instance failures. You are required to launch the application in the most cost-effective way.

Which type of EC2 instance will meet your requirements?

- A. Spot Instances
- B. On-Demand instances
- C. Reserved instances
- D. Dedicated instances

[Check answer to Question #180](#)

Question #181

A technology company is building a new cryptocurrency trading platform that allows buying and selling of Bitcoin, Ethereum, XRP, Ripple 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 defines all 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 was disappointed that you are just slacking off at your job.

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. A storage location for the code of your application
- B. Provides highly durable and scalable data storage
- C. Using CloudFormation itself is free, including the AWS resources that have been created.

- D. Allows you to model your entire infrastructure in a text file
- E. Enables modeling, provisioning, and version-controlling of your entire AWS infrastructure

[Check answer to Question #181](#)

Question #182

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. EFS
- B. S3
- C. EBS
- D. Glacier

[Check answer to Question #182](#)

Question #183

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. Use DynamoDB Auto Scaling
- B. Create an SQS queue in front of the DynamoDB table.
- C. Integrate an Application Load Balancer with your DynamoDB table.
- D. Add the DynamoDB table to an Auto Scaling Group.

[Check answer to Question #183](#)

Question #184

You are working as a Solutions Architect for a leading data analytics company in which you are tasked to process real-time streaming data of your users across the globe. This will enable you to track and analyze globally-distributed user activity on your website and mobile applications, including click stream analysis. Your cloud architecture should process the data in close geographical proximity to your users and to respond to user requests at low latencies.

Which of the following options is the most ideal solution that you should implement?

- A. 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.
- B. 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.
- 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 Amazon Athena and durably store the results to an Amazon S3 bucket.
- D. 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.

[Check answer to Question #184](#)

Question #185

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. Enable Cross-Region Replication.
- C. Create a new S3 bucket in another region and configure Cross-Account Access to the bucket located in us-east-1.
- D. Copy the S3 bucket to an EBS-backed EC2 instance.

[Check answer to Question #185](#)

Question #186

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 must 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. S3 Select, Amazon Athena, Amazon Redshift Spectrum
- B. Amazon X-Ray, Amazon Neptune, DynamoDB
- C. Amazon Glue, Glacier Select, Amazon Redshift
- D. S3 Select, Amazon Neptune, DynamoDB DAX

[Check answer to Question #186](#)

Question #187

To save cost, a company decided to change their third-party data analytics tool to a cheaper solution. They sent a full data export on a CSV file which contains all 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 a standard SQL?

- A. Use a migration tool to load the CSV export file from S3 to a database which is designed for online analytic processing (OLAP) such as AWS RedShift. Run some queries once the data has been loaded to complete your validation.
- B. 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.
- C. 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.
- D. To be able to run SQL queries, use AWS Athena to analyze the export data file in S3.

[Check answer to Question #187](#)

Question #188

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. Configure AWS Config to trigger an evaluation that will check the compliance for a user's password periodically.
- 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. 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.

[Check answer to Question #188](#)

Question #189

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 must 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. Invoke the Lambda functions using SNS each time that the ECS Cluster successfully processed financial data.
- B. Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function.

- C. Use CloudWatch Alarms to trigger the Lambda function whenever a new entry is created in the DynamoDB table.
- D. Use Systems Manager Automation to detect new entries in the DynamoDB table then automatically invoke the Lambda function for processing.

[Check answer to Question #189](#)

Question #190

You have 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 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.
- B. 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.
- 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 calls a Lambda function that invokes an action to restart the EC2 instance.
- D. 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.

[Check answer to Question #190](#)

Question #191

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 if 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. Amazon SQS
- B. Amazon LightSail
- C. Amazon SNS
- D. AWS CloudFormation

[Check answer to Question #191](#)

Question #192

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":"DirectoryTechradio1234", "Effect":"Allow", "Action": [ "ds:*" ], "Resource": "arn:aws:ds:us-east-1:987654321012:directory/d-1234567890" }, { "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 if the resource contains the directory ID: DirectoryTechradio1234
- B. Allows all AWS Directory Service (ds) calls if the resource contains the directory ID: 987654321012

- C. Allows all AWS Directory Service (ds) calls if the resource contains the directory name of: DirectoryTechradio1234
- D. Allows all AWS Directory Service (ds) calls if the resource contains the directory ID: d-1234567890

[Check answer to Question #192](#)

Question #193

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 the AWS resources that they are using.

In this scenario, which of the following will incur costs? (Select TWO.)

- A. EBS Volumes attached to stopped EC2 Instances
- B. A stopped On-Demand EC2 Instance
- C. A running EC2 Instance
- D. Public Data Set
- E. Using an Amazon VPC

[Check answer to Question #193](#)

Question #194

You have 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 the 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. A single On-Demand Amazon EC2 instance for both storing and processing the log files

- C. Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.
- D. Amazon S3 Glacier for storing the application log files and Spot EC2 Instances for processing them.

[Check answer to Question #194](#)

Question #195

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 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.
- B. 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.
- C. Deploy the web and application tier instances to a public subnet and then allocate an Elastic IP address to each EC2 instance.
- D. Deploy the web and application tier instances to a private subnet and then allocate an Elastic IP address to each EC2 instance.

[Check answer to Question #195](#)

Question #196

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

[Check answer to Question #196](#)

Question #197

You are a Solutions Architect for a global news company. You are configuring a fleet of EC2 instances in a subnet which currently is in a VPC with an Internet gateway attached. All these EC2 instances can be accessed from the Internet. You then launch another subnet and launch an EC2 instance in it, however you are not able to access the EC2 instance from the Internet.

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

- A. The Amazon EC2 instance does not have a public IP address associated with it.
- B. The Amazon EC2 instance does not have an attached Elastic Fabric Adapter (EFA).
- C. The Amazon EC2 instance is not a member of the same Auto Scaling group.
- D. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the Internet gateway.
- E. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the customer gateway (CGW).

[Check answer to Question #197](#)

Question #198

You are working for a large financial firm in the country. They have an AWS environment which contains several Reserved EC2 instances hosted in a web application that has been decommissioned last week. To save cost, 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. Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.
- B. Stop the Reserved instances as soon as possible.
- C. Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires.
- D. Contact AWS to cancel your AWS subscription.
- E. Go to the Amazon.com online shopping website and sell the Reserved instances.

[Check answer to Question #198](#)

Question #199

You are setting up the 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, you have deployed your AWS resources to multiple AWS Regions. You need to use Route 53 and configure it to set all your resources to be available all the time as much as possible. When a resource becomes unavailable, your 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 you should use in this scenario?

- A. Configure an Active-Active Failover with One Primary and One Secondary Resource.

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

[Check answer to Question #199](#)

Question #200

An Architect is managing a data analytics application which exclusively uses Amazon S3 as its data storage. For the past few weeks, the application works as expected until a new change was implemented to increase the rate at which the application updates its data. There have been reports that outdated data intermittently appears when the application accesses objects from S3 bucket. The development team investigated the application logic and didn't find any issues.

Which of the following is the MOST likely cause of this issue?

- A. The data analytics application is designed to fetch parts of objects from the S3 bucket using a range header.
- B. The data analytics application is designed to update its data with an object-locking mechanism.
- C. The data analytics application is designed to fetch objects from the S3 bucket using parallel requests.
- D. The data analytics application is designed to use atomic updates across object keys.

[Check answer to Question #200](#)

Question #201

You are a new Solutions Architect in your company. Upon checking the existing Inbound Rules of your Network ACL, you saw this configuration:

Rule#: 100, Type: All Traffic, Protocol: ALL, Port Range: ALL, Source: 0.0.0.0/0 Allow

Rule#: 100, Type: Custom TCP Rule, Protocol: TCP(6), Port Range: 4000, Source: 120.230.28.100/32 DENY

Rule#: *, Type: All Traffic, Protocol: ALL, Port Range: ALL, Source: 0.0.0.0/0 DENY

If a computer with an IP address of 110.238.109.37 sends a request to your VPC, what will happen?

- A. It will be denied.
- B. Initially, it will be allowed and then after a while, the connection will be denied.
- C. It will be allowed.
- D. Initially, it will be denied and then after a while, the connection will be allowed.

[Check answer to Question #201](#)

Question #202

Your 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 afterwards, purge the logs.

What should you do to accomplish this requirement?

- A. Create a new IAM policy for the Amazon S3 bucket that automatically deletes the logs after a month
- B. Add a new bucket policy on the Amazon S3 bucket.
- C. Enable CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data
- D. Configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month

[Check answer to Question #202](#)

Question #203

You are the Solutions Architect for your company's AWS account of approximately 300 IAM users. They have a new company policy that will change the access of 100 of the IAM users to have a sort of access to Amazon S3 buckets.

What will you do to avoid the time-consuming task of applying the policy at the individual user?

- A. Create a new IAM group and then add the users that require access to the S3 bucket. Afterwards, apply the policy to IAM group.
- B. Create a new IAM role and add each user to the IAM role.
- C. Create a new policy and apply it to multiple IAM users using a shell script.
- D. Create a new S3 bucket access policy with unlimited access for each IAM user.

[Check answer to Question #203](#)

Question #204

You are working for a large IT consultancy company as a Solutions Architect. One of your 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 you use to meet this requirement?

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

[Check answer to Question #204](#)

Question #205

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

[Check answer to Question #205](#)

Question #206

A VPC has a non-default subnet which has four On-Demand EC2 instances that can be accessed over the Internet. Using the AWS CLI, you launched a fifth instance that uses the same subnet, Amazon Machine Image (AMI), and security group which are being used by the other instances. Upon testing, you are not able to access the new instance.

Which of the following is the most suitable solution to solve this problem?

- A. Set up a NAT gateway to allow access to the fifth EC2 instance.
- B. Enable AWS Transfer for SFTP to allow the incoming traffic to the fifth EC2 Instance.
- C. Associate an Elastic IP address to the fifth EC2 instance.
- D. Include the fifth EC2 instance to the Placement Group of the other four EC2 instances and enable Enhanced Networking.

[Check answer to Question #206](#)

Question #207

Your company is in a hurry of deploying their new web application written in NodeJS to AWS. As the Solutions Architect of the company, you were assigned to do the deployment without worrying about the underlying infrastructure that runs the application.

Which service will you use to easily deploy and manage your new web application in AWS?

- A. AWS CodeCommit
- B. AWS CloudFormation
- C. Amazon CloudFront
- D. AWS Elastic Beanstalk

[Check answer to Question #207](#)

Question #208

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. Use larger instances for your application with an attached Elastic Fabric Adapter (EFA).
- 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. Set up Amazon Aurora Serverless for on-demand, auto-scaling configuration of your EC2 Instances and enable Amazon Aurora Parallel Query feature for faster analytical queries over your current data.

- 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.

[Check answer to Question #208](#)

Question #209

You were recently promoted to a technical lead role in your DevOps team. Your company has an existing VPC which is quite unutilized for the past few months. The business manager instructed you to integrate your on-premises data center and your VPC. You explained the list of tasks that you'll be doing and mentioned about a 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 provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- D. 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.

[Check answer to Question #209](#)

Question #210

You are a new Solutions Architect working for a financial company. Your 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 you can provide to them?

- A. Use Amazon SWF.
- 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.

[Check answer to Question #210](#)

Question #211

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

[Check answer to Question #211](#)

Question #212

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. Provides synchronous replication and automatic failover in the case of Availability Zone service failures.
- C. Allows both read and write operations on the read replica to complement the primary database.
- D. It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.
- E. Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.

[Check answer to Question #212](#)

Question #213

Your IT Manager instructed you to set up a bastion host in the cheapest, most secure way, and that you should be the only person that can access it via SSH.

Which of the following steps would satisfy your IT Manager's request?

- A. Set up a large EC2 instance and a security group which only allows access on port 22
- B. Set up a small EC2 instance and a security group which only allows access on port 22 via your IP address
- C. Set up a small EC2 instance and a security group which only allows access on port 22
- D. Set up a large EC2 instance and a security group which only allows access on port 22 via your IP address

[Check answer to Question #213](#)

Question #214

You have an On-Demand EC2 instance located in a subnet in AWS which hosts a web application. The security group attached to this EC2 instance has the following Inbound Rules:

Type: SSH, Protocol: TCP, Port Range: 22, Source: 0.0.0.0/0

The Route table attached to the VPC is shown below.

Destination: 10.0.0.0/27, Target: local, Status: Active, Propagated: No

Destination: 0.0.0.0/0, Target: igw-b2196sd, Status: Active, Propagated: No

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.

Which of the below steps would resolve the issue?

- A. In the Route table, add this new route entry: 0.0.0.0 -> igw-b2196sd
- B. In the Security Group, add an Inbound HTTP rule.
- C. In the Security Group, remove the SSH rule.
- D. In the Route table, add this new route entry: 10.0.0.0/27 -> local

[Check answer to Question #214](#)

Question #215

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

[Check answer to Question #215](#)

Question #216

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 EFS
- B. AWS Fargate
- C. Amazon EKS
- D. Amazon EBS

[Check answer to Question #216](#)

Question #217

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. 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.
- 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. 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.

[Check answer to Question #217](#)

Question #218

You are working as an IT Consultant for a large investment bank that generates large financial datasets with millions of rows. The data must be stored 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 which 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 Redshift
- B. Amazon RDS
- C. DynamoDB
- D. Amazon Aurora

[Check answer to Question #218](#)

Question #219

You are working as a Solutions Architect for a multinational financial firm. They have 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. FTP
- C. AWS Direct Connect
- D. Amazon S3 Transfer Acceleration

[Check answer to Question #219](#)

Question #220

You are working as a Solutions Architect for a tech company where you are instructed to build a web architecture using On-Demand EC2 instances and a database in AWS. However, due to budget constraints, the company instructed you 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 database service in AWS is best to use in this scenario?

- A. RDS

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

[Check answer to Question #220](#)

Question #221

A music 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 on Amazon S3. The company has a policy that any data stored outside its own data center must be encrypted. This way, even if the data is hacked, nobody will be able to read it without the encryption keys. Which of the following methods can achieve this? (Select TWO.)

- A. Use SSL to encrypt the data while in transit to Amazon S3.
- B. Use Amazon S3 server-side encryption with customer-provided keys.
- C. Use Amazon S3 server-side encryption with EC2 key pair.
- D. Encrypt the data on the client-side using your own master key then upload the data to Amazon S3.
- E. Use Amazon S3 bucket policies to restrict access to the data at rest.

[Check answer to Question #221](#)

Question #222

You are working as a Cloud Engineer for a top aerospace engineering firm. One of your tasks is to set up a document storage system using S3 for all the engineering files. In Amazon S3, which of the following statements are true? (Select TWO.)

- A. You can only store ZIP or TAR files in S3.
- B. The total volume of data and number of objects you can store are unlimited.
- C. The largest object that can be uploaded in a single PUT is 5 TB.
- D. S3 is an object storage service that provides file system access semantics (such as strong consistency and file locking), and

concurrently-accessible storage.

- E. The largest object that can be uploaded in a single PUT is 5 GB.

[Check answer to Question #222](#)

Question #223

An online stock 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 any time 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. Retrieve the data using Amazon Glacier Select.
- B. Use Expedited Retrieval to access the financial data.
- C. Purchase provisioned retrieval capacity.
- D. Specify a range, or portion, of the financial data archive to retrieve.
- E. Use Bulk Retrieval to access the financial data.

[Check answer to Question #223](#)

Question #224

You are working as a Solutions Architect for a leading airline company where you are building a decoupled application in AWS using EC2, Auto Scaling group, S3 and SQS. You 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. FIFO queues provide exactly-once processing.
- B. Amazon SQS can help you build a distributed application with decoupled components.
- 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.

[Check answer to Question #224](#)

Question #225

You are unable to connect to your new EC2 instance via SSH from your home computer, which you have recently deployed. However, you were able to successfully access other existing instances in your VPC without any issues.

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

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

[Check answer to Question #225](#)

Question #226

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-love-kolkata.com, i-love-mumbai.com, i-love-bengaluru.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 every time 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 cost-effective 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.

[Check answer to Question #226](#)

Question #227

Your company has recently deployed a new web application which uses a serverless-based architecture in AWS. Your manager instructed you to implement CloudWatch metrics to monitor your systems more effectively. You know that Lambda automatically monitors functions on your behalf and reports metrics through Amazon CloudWatch.

In this scenario, what types of data do these metrics monitor? (Select TWO.)

- A. IteratorSize
- B. Invocations
- C. ApproximateAgeOfOldestMessage
- D. Async Delivery Failures

E. ReservedConcurrentExecutions

[Check answer to Question #227](#)

Question #228

You are a Solutions Architect for a major TV network. They have a web application running on eight Amazon T3 EC2 instances, consuming about 55% of resources on each instance. You are using Auto Scaling to make sure that eight instances are always running . The number of requests that this application processes are consistent and do not experience spikes. Your manager always instructed you to ensure high availability of this web application to avoid any loss of revenue. You want the load to be distributed evenly between all instances.

You also want to use the same Amazon Machine Image (AMI) for all EC2 instances. How will you be able to achieve this?

- A. Deploy four EC2 instances with Auto Scaling in one region and four in another region behind an Amazon Elastic Load Balancer.
- B. Deploy two EC2 instances with Auto Scaling in four regions behind an Amazon Elastic Load Balancer.
- C. Deploy eight EC2 instances with Auto Scaling in one Availability Zone 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.

[Check answer to Question #228](#)

Question #229

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 s3:ObjectRemoved:Delete 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:ObjectAdded:* and s3:ObjectRemoved:* 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:ObjectCreated:* and ObjectRemoved:DeleteMarkerCreated 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 ObjectRemoved:DeleteMarkerCreated event types to SQS and SNS.

[Check answer to Question #229](#)

Question #230

An online job site is using NGINX for its application servers hosted in EC2 instances and MongoDB Atlas for its database-tier. MongoDB Atlas is a fully automated third-party cloud service which is not provided by AWS, but supports VPC peering to connect to your VPC.

Which of the following items are invalid VPC peering configurations?
(Select TWO.)

- A. One VPC Peered with two VPCs using longest prefix match
- B. Two VPCs peered to a specific CIDR block in one VPC
- C. One to one relationship between two Virtual Private Cloud networks

- D. Transitive Peering
- E. Edge to Edge routing via a gateway

[Check answer to Question #230](#)

Question #231

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

[Check answer to Question #231](#)

Question #232

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

- B. Use an Amazon CloudFront service for distributing both static and dynamic content.
- C. Use AWS Shield and AWS WAF.
- D. Use Dedicated EC2 instances to ensure that each instance has the maximum performance possible.
- E. Use an Application Load Balancer with Auto Scaling groups for your EC2 instances then restrict direct Internet traffic to your Amazon RDS database by deploying to a private subnet.

[Check answer to Question #232](#)

Question #233

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 Snowball
- D. Use AWS Import/Export

[Check answer to Question #233](#)

Question #234

Your customer has clients 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 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 you implement to meet the above requirements? (Select TWO.)

- A. Use AWS App Mesh to ensure that only their client can access the files.
- B. Use AWS Cloud Map 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. Require the users to access the private content by using special CloudFront signed URLs or signed cookies.
- E. 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.

[Check answer to Question #234](#)

Question #235

You are a new Solutions Architect in your department, and you have created 7 CloudFormation templates. Each template has been defined for a specific purpose. What determines the cost of using these new CloudFormation templates?

- A. \$2.50 per template per month
- B. It depends on the region where you will deploy.
- C. CloudFormation templates are free but you are charged for the underlying resources it builds.
- D. The length of time it takes to build the architecture with CloudFormation

[Check answer to Question #235](#)

Question #236

You are working for an insurance firm as their Senior Solutions Architect. The firm has an application which processes thousands of customer data stored in an Amazon MySQL database with Multi-AZ deployments configuration for high availability in case of downtime. For the past few days, you noticed an increasing trend of read and write operations, which is increasing the latency of the queries to your database. You are planning to use the standby database instance to balance the read and write operations from the primary instance.

When running your primary Amazon RDS Instance as a Multi-AZ deployment, can you use the standby instance for read and write operations?

- A. Only with Microsoft SQL Server-based RDS
- B. No
- C. Yes
- D. Only for Oracle RDS instances

[Check answer to Question #236](#)

Question #237

You are working for a FinTech startup as their AWS Solutions Architect. You deployed an application on different EC2 instances with Elastic IP addresses attached for easy DNS resolution and configuration. These servers are 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 an EC2 instance with an associated Elastic IP 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. There will be no changes.
- D. All data on the attached instance-store devices will be lost.
- E. The Elastic IP address is disassociated with the instance.

[Check answer to Question #237](#)

Question #238

You are working for a Social Media Analytics company as its head data analyst. You want to collect gigabytes of data per second from websites and social media feeds to gain insights from data generated by its 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.

Which AWS service can you use to collect and process large streams of data records in real time?

- A. Amazon Kinesis Data Streams
- B. Amazon S3
- C. Amazon SWF
- D. Amazon Redshift

[Check answer to Question #238](#)

Question #239

You are working for an investment bank as their IT Consultant. You are working with their IT team to handle the launch of their 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, you are 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. Use AWS Shield and WAF
- 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. Create an EBS Snapshot

[Check answer to Question #239](#)

Question #240

A company is using a custom shell script to automate the deployment and management of their EC2 instances. The script is using various AWS CLI commands such as revoke-security-group-ingress, revoke-security-group-egress, run-scheduled-instances and many others.

In the shell script, what does the revoke-security-group-ingress command do?

- A. Removes one or more security groups from a rule.
- B. Removes one or more ingress rules from a security group.
- C. Removes one or more security groups from an Amazon EC2 instance.
- D. Removes one or more egress rules from a security group.

[Check answer to Question #240](#)

Question #241

You currently have an Augment Reality (AR) mobile game which 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. 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.
- C. Use API Gateway in conjunction with Lambda and turn on the caching on frequently accessed data and enable DynamoDB global replication.
- D. 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.
- E. Configure CloudFront with DynamoDB as the origin; cache frequently accessed data on client device using ElastiCache.

[Check answer to Question #241](#)

Question #242

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. Scheduled Reserved Instances
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

[Check answer to Question #242](#)

Question #243

You are a Solutions Architect in your company where you are tasked to set up a cloud infrastructure. In the planning, it was discussed that you will need two EC2 instances which 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

[Check answer to Question #243](#)

Question #244

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. 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.
- D. 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.

[Check answer to Question #244](#)

Question #245

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. Do nothing. You can start directly launching EC2 instances in the Auto Scaling group with the same launch configuration.
- B. Create a new target group.
- C. Create a new target group and launch configuration.
- D. Create a new launch configuration.

[Check answer to Question #245](#)

Question #246

You are a Solutions Architect working for an aerospace engineering company which recently adopted a hybrid cloud infrastructure with AWS. One of your tasks is to launch a VPC with both public and private subnets for their EC2 instances as well as their database instances respectively.

Which of the following statements are true regarding Amazon VPC subnets? (Select TWO.)

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

[Check answer to Question #246](#)

Question #247

You are working for a startup company that has resources deployed on the AWS Cloud. Your company 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. AWS CloudTrail
- B. Amazon EC2
- C. Amazon CloudWatch
- D. Amazon VPC

[Check answer to Question #247](#)

Question #248

You have a VPC that has a CIDR block of 10.31.0.0/27 which is connected to your 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 you set up the serverless architecture and connected Lambda function to your VPC, you noticed that there is an increase in invocation errors with EC2 error types such as EC2ThrottledException on certain times of the day.

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

- A. The attached IAM execution role of your function does not have the necessary permissions to access the resources of your VPC.
- B. The associated security group of your function does not allow outbound connections.
- C. Your VPC does not have a NAT gateway.
- D. Your VPC does not have enough subnet ENIs or subnet IPs.
- E. 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.

[Check answer to Question #248](#)

Question #249

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

[Check answer to Question #249](#)

Question #250

You installed sensors to track the number of visitors that goes to 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 your S3 bucket is not receiving all 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, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream.
- B. By default, Amazon S3 stores the data for 1 day and moves it to Amazon Glacier.
- C. Your AWS account was hacked, and someone has deleted some data in your Kinesis stream.
- D. There is a problem in the sensors. They probably had some intermittent connection hence; the data is not sent to the stream.

[Check answer to Question #250](#)

Question #251

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

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

[Check answer to Question #251](#)

Question #252

Your web application is relying entirely on slower disk-based databases, causing it to perform slowly. To improve its performance, you integrated an in-memory data store to your web application using ElastiCache. How does Amazon ElastiCache improve database performance?

- A. 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.
- B. It securely delivers data to customers globally with low latency and high transfer speeds.
- C. It reduces the load on your database by routing read queries from your applications to the Read Replica.
- D. By caching database query results.

[Check answer to Question #252](#)

Question #253

Your manager has asked you 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 real-time ranking.

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

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

[Check answer to Question #253](#)

Question #254

You are working as a Solutions Architect for an aerospace manufacturer which heavily uses AWS. They are running a prototype high performance computing (HPC) cluster that spans multiple EC2 instances across multiple Availability Zones, which processes various wind simulation models.

Currently, you are experiencing a slowdown in your applications and upon further investigation, it was discovered that it was due to latency issues.

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

- A. Set up a cluster placement group within a single Availability Zone in the same AWS Region.
- B. Use EC2 Dedicated Instances.
- C. Set up a spread placement group across multiple Availability Zones in multiple AWS Regions.
- D. Set up AWS Direct Connect connections across multiple Availability Zones for increased bandwidth throughput and more consistent network experience.

[Check answer to Question #254](#)

Question #255

In your VPC, you have a Classic Load Balancer distributing traffic to 2 running EC2 instances in ap-southeast-1a AZ and 8 EC2 instances in ap-southeast-1b AZ. However, you noticed that half of your incoming traffic goes to ap-southeast-1a AZ which over-utilize its 2 instances but underutilize the other 8 instances in the other AZ.

What could be the most likely cause of this problem?

- A. The security group of the EC2 instances does not allow HTTP traffic.
- B. The Classic Load Balancer listener is not set to port 80.
- C. The Classic Load Balancer listener is not set to port 22.
- D. Cross-Zone Load Balancing is disabled.

[Check answer to Question #255](#)

Question #256

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 the incoming read requests equally to the two Read Replicas?

- A. Use the built-in Cluster endpoint of the Amazon Aurora database.
- B. Use the built-in Reader endpoint of the Amazon Aurora database.
- C. Enable Amazon Aurora Parallel Query.
- D. Create a new Network Load Balancer to evenly distribute the read queries to the Read Replicas of the Amazon Aurora database.

[Check answer to Question #256](#)

Question #257

A leading media company has an application hosted in an EBS-backed EC2 instance which uses Simple Workflow Service (SWF) to handle its sequential background jobs. The application works well in production and your manager asked you to also implement the same solution to other areas of their business.

In which other scenarios can you use both Simple Workflow Service (SWF) and Amazon EC2 as a solution? (Select TWO.)

- A. For applications that require a message queue.
- B. For a distributed session management for your mobile application.
- C. Orchestrating the execution of distributed business processes.
- D. Managing a multi-step and multi-decision checkout process of an e-commerce mobile app.
- E. For web applications that require content delivery networks.

[Check answer to Question #257](#)

Question #258

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 DependsOn attribute in the CloudFormation template. Send a success signal after the applications are installed and configured using the cfn-init helper script.

- B. 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.
- C. 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.
- D. 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.

[Check answer to Question #258](#)

Question #259

You are working for a large telecommunications company where you need to run analytics against all combined log files from your 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 EC2 with EBS volumes for storing and analyzing the log files.
- C. Amazon DynamoDB for storing and EC2 for analyzing the logs.
- D. Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.

[Check answer to Question #259](#)

Question #260

You are working for a large financial firm and you are instructed to set up a Linux bastion host. It will 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. Network ACL Inbound Rule: Protocol TCP, Port Range-22, Source 175.45.116.100/0
- B. Network ACL Inbound Rule: Protocol UDP, Port Range 22, Source 175.45.116.100/32
- C. Security Group Inbound Rule: Protocol UDP, Port Range 22, Source 175.45.116.100/32
- D. Security Group Inbound Rule: Protocol TCP. Port Range 22, Source 175.45.116.100/32

[Check answer to Question #260](#)

Question #261

Your customer 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 for processing before it is stored in an S3 bucket. Afterwards, if the upload was successful, the application will return a prompt telling the user that the upload is 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 reply, in the most cost-effective manner?

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

[Check answer to Question #261](#)

Question #262

You developed a web application and deployed it on a fleet of EC2 instances, which is using 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 you developed the application, you can easily resolve the issue, but you need to send a communication to the users on the issue.

What information will you provide and what will happen to the unprocessed messages?

- A. Tell the users that unfortunately, they must resubmit all the requests again.
- B. Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted.
- C. Tell the users that unfortunately, they must resubmit all of the requests since the queue would not be able to process the 10,000 messages together.
- D. Tell the users that the application will be operational shortly however, requests sent over three days ago will need to be resubmitted.

[Check answer to Question #262](#)

Question #263

You have a static corporate website hosted in a standard S3 bucket and a new web domain name which 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. The S3 bucket must be in the same region as the hosted zone
- E. A registered domain name

[Check answer to Question #263](#)

Question #264

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 Snowmobile
- B. Amazon S3 Multipart Upload
- C. AWS Snowball Edge
- D. AWS Direct Connect

[Check answer to Question #264](#)

Question #265

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 instances 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.

[Check answer to Question #265](#)

Question #266

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

[Check answer to Question #266](#)

Question #267

You are working for a commercial bank as an AWS Infrastructure Engineer handling the forex trading application of the bank. You have an Auto

Scaling group of EC2 instances that allow your company to cope up with the current demand of traffic and achieve cost-efficiency. You 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 your system from unintended slowdown or unavailability.

Which of the following statements are true regarding the cooldown period? (Select TWO.)

- A. Its default value is 600 seconds.
- B. It ensures that before the Auto Scaling group scales out, the EC2 instances have an ample time to cooldown.
- C. It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
- D. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.
- E. Its default value is 300 seconds.

[Check answer to Question #267](#)

Question #268

You are a Solutions Architect of a multi-national gaming company which develops video games for PS4, Xbox One and Nintendo Switch consoles, plus several mobile games for Android and iOS. Due to the wide range of their products and services, you proposed that they use API Gateway.

What are the key features of API Gateway that you can tell your client? (Select TWO.)

- A. Provides you with static anycast IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions.
- B. Enables you to build RESTful APIs and WebSocket APIs that are optimized for serverless workloads.
- C. It automatically provides a query language for your APIs like GraphQL.
- D. 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.
- E. You pay only for the API calls you receive, and the amount of data transferred out.

[Check answer to Question #268](#)

Question #269

Your fellow AWS Engineer has created a new Standard-class S3 bucket to store financial reports that are not frequently accessed but should be immediately available when an auditor requests it. To save costs, you 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. It is designed for data that requires rapid access when needed.
- B. Ideal to use for data archiving.
- C. It is the best storage option to store noncritical and reproducible data
- D. It is designed for data that is accessed less frequently.
- E. It provides high latency and low throughput performance

[Check answer to Question #269](#)

Question #270

You have a new, 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. Enable failover to an application hosted in an on-premises data center.
- C. Duplicate the exact application architecture in another region and configure DNS weight-based routing.
- D. Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution.

[Check answer to Question #270](#)

Question #271

Your client is an insurance company that utilizes SAP HANA for their day-to-day ERP operations. Since you can't migrate this database due to customer preferences, you need to integrate it with your current AWS workload in your VPC in which you are required to establish a site-to-site VPN connection.

What needs to be configured outside of the VPC for you to have a successful site-to-site VPN connection?

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

[Check answer to Question #271](#)

Question #272

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 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.
- B. Launch 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.
- C. 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.
- D. Launch 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.

[Check answer to Question #272](#)

Question #273

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 does not have a public IP address associated with it.
- B. The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway.

- C. The EC2 instance does not have a private IP address associated with it.
- D. The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway.

[Check answer to Question #273](#)

Question #274

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.

[Check answer to Question #274](#)

Question #275

You have set up a VPC with public subnet and an Internet gateway. You set up an EC2 instance with a public IP as well. However, you are still not able to connect to the instance via the Internet. You checked its associated security group and it seems okay.

What should you do to ensure you can connect to the EC2 instance from the Internet?

- A. Set a Secondary Private IP Address to the EC2 instance.
- B. Set an Elastic IP Address to the EC2 instance.

- C. Check the main route table and ensure that the right route entry to the Internet Gateway (IGW) is configured.
- D. Check the CloudWatch logs as there must be some issue in the EC2 instance.

[Check answer to Question #275](#)

Question #276

Your company just recently adopted a hybrid architecture that integrates their on-premises data center to their AWS cloud. You are assigned to configure the VPC as well as to implement the required IAM users, IAM roles, IAM groups and IAM policies. In this scenario, what is a 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. Use the principle of least privilege which means granting only the least number of people with full root access.
- C. Use the principle of least privilege which means granting only the permissions required to perform a task.
- D. Grant all permissions to any EC2 user.

[Check answer to Question #276](#)

Question #277

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 RDS to utilize both on-premises servers and EC2 instances for your decoupled application
- B. Use Amazon Simple Decoupling Service to utilize both on-premises servers and EC2 instances for your decoupled application

- C. Use SQS 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 SWF to utilize both on-premises servers and EC2 instances for your decoupled application

[Check answer to Question #277](#)

Question #278

A San Francisco-based tech startup is building a cross-platform mobile app that can notify the user with upcoming astronomical events such as eclipses, blue moon, novae or a meteor shower. Your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK and Amazon Cognito. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito.

Which of the following is returned for the user to provide a set of temporary, limited-privilege AWS credentials?

- A. Cognito ID
- B. Cognito API
- C. Cognito SDK
- D. Cognito Key Pair

[Check answer to Question #278](#)

Question #279

A messaging application in ap-northeast-1 region uses m4.2xlarge instance to accommodate 75 percent of users from Tokyo and Seoul. It uses a cheaper m4.large instance in ap-southeast-1 to accommodate the rest of users from Manila and Singapore.

As a Solutions Architect, what routing policy should you use to route traffic to your instances based on the location of your users and instances?

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

[Check answer to Question #279](#)

Question #280

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

[Check answer to Question #280](#)

Question #281

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

[Check answer to Question #281](#)

Question #282

You are a Solutions Architect working with a company that uses Chef Configuration management in their datacenter. Which service is designed to let the customer leverage existing Chef recipes in AWS?

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

[Check answer to Question #282](#)

Question #283

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 a DynamoDB table.

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

[Check answer to Question #283](#)

Question #284

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 that data stored on the S3 bucket must be encrypted.

What is the best option to do this? (Select TWO.)

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

[Check answer to Question #284](#)

Question #285

You are building a cloud infrastructure where you have EC2 instances that require access to various AWS services such as S3 and Redshift. You will also need to provision access to system administrators so they can deploy and test their changes. Which configuration should be used to ensure that the access to your resources are secured and not compromised? (Select TWO.)

- A. Enable Multi-Factor Authentication.

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

[Check answer to Question #285](#)

Question #286

You have 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, you noticed that there are a lot of occurrences where a shard iterator expires unexpectedly. Upon checking, you 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. Increase the write capacity assigned to the shard table.
- B. Use Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream.
- C. Upgrade the storage capacity of the DynamoDB table.
- D. Enable In-Memory Acceleration with DynamoDB Accelerator (DAX).

[Check answer to Question #286](#)

Question #287

You are working for a University as their AWS Consultant. They want to have a disaster recovery strategy in AWS for mission-critical applications after suffering a disastrous outage wherein they lost student and employee records. They don't want this to happen again but at the same time want to minimize the monthly costs. You are instructed to set up a minimal version of the application that is always available in case of any outages. The DR site should only run the most critical core elements of your system in AWS to save cost which can be rapidly upgraded to a full-scale

production environment in the event of system outages. Which of the following disaster recovery architectures is the most cost-effective type to use in this scenario?

- A. Warm Standby
- B. Backup & Restore
- C. Pilot Light
- D. Multi-Site

[Check answer to Question #287](#)

Question #288

Your company has a top priority requirement to monitor a few database metrics and then afterwards, send email notifications to the Operations team in case there is an issue.

Which AWS services can accomplish this requirement? (Select TWO.)

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

[Check answer to Question #288](#)

Question #289

You are working as a Cloud Consultant for a government agency with a mandate of improving traffic planning, maintenance of roadways and preventing accidents. There is a need to manage 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 said devices to your cloud-based applications?

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

[Check answer to Question #289](#)

Question #290

You work for a leading university as an AWS Infrastructure Engineer and as a professor to aspiring AWS architects. To familiarize your students with AWS, you gave them a project to host their applications to an EC2 instance. One of your students created an instance to host their online enrollment system project but is having a hard time connecting to their newly created EC2 instance. Your students have explored all the troubleshooting guides by AWS and narrowed it down to login issues.

Which of the following can you use to log into an EC2 instance?

- A. EC2 Connection Strings
- B. Key Pairs
- C. Access Keys
- D. Custom EC2 password

[Check answer to Question #290](#)

Question #291

In Elastic Load Balancing, there are various security features that you can use such as Server Order Preference, Predefined Security Policy, Perfect Forward Secrecy and many others. Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data using a unique random session key. This prevents the

decoding of captured data, even if the secret long-term key is compromised.

Perfect Forward Secrecy is used to offer SSL/TLS cipher suites for which two AWS services?

- A. EC2 and S3
- B. CloudTrail and CloudWatch
- C. CloudFront and Elastic Load Balancing
- D. Trusted Advisor and GovCloud

[Check answer to Question #291](#)

Question #292

You are instructed by your manager to set up a bastion host in your Amazon VPC and it should only be accessed from the corporate data center via SSH.

What is the best way for you to achieve this?

- A. Create a small EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.
- B. 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.
- C. 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.
- D. Create a large EC2 instance with a security group which only allows access on port 22 using your own pre-configured password.

[Check answer to Question #292](#)

Question #293

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

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

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

[Check answer to Question #293](#)

Question #294

You are a Solutions Architect working for a large insurance company that deployed their production environment on a custom Virtual Private Cloud in AWS with a default configuration. The VPC consists of two private subnets and one public subnet. Inside the public subnet is a group of EC2 instances which are created by an Auto Scaling group and all the instances are in the same Security Group. Your development team has created a new application which will be accessed by mobile devices via a custom port. This application has been deployed to the production environment and you need to open this port globally to the Internet.

Which of the following is the correct procedure to meet this requirement?

- A. Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port immediately.
- B. Open the custom port on the Security Group. Your EC2 instances will be able to use this port after 60 minutes.
- C. Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port after a reboot.

- D. Open the custom port on the Security Group. Your EC2 instances will be able to use this port immediately.

[Check answer to Question #294](#)

Question #295

As part of the Business Continuity Plan of your company, your IT Director instructed you to set up an automated backup of all 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 your EBS Volumes?

- A. Use an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots.
- C. 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.
- D. 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.

[Check answer to Question #295](#)

Question #296

You work for an Intelligence Agency as its Principal Consultant developing a missile tracking application, which is hosted on both development and production AWS accounts. Alice, 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 acts as temporary security credentials to allow access to your AWS resources?

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

[Check answer to Question #296](#)

Question #297

You are working for an advertising company as their Senior Solutions Architect handling the S3 storage data. Your company has terabytes of data sitting on AWS S3 standard storage class, which accumulates significant operational costs. The management wants to cut down on the cost of their cloud infrastructure, so you were instructed to switch to Glacier to lessen the cost per GB storage.

Which use case is the Amazon Glacier storage service primarily used for? (Select TWO.)

- A. Used for active database storage
- B. Storing Data archives
- C. Storing cached session data
- D. Used as a data warehouse
- E. Storing infrequently accessed data

[Check answer to Question #297](#)

Question #298

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 Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic.
- B. 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).
- C. It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS
- D. Use an Elastic IP and upload multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager.

[Check answer to Question #298](#)

Question #299

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. The sqsSendMessage attribute of the SQS queue is configured to 50.
- B. There is a bug in the application.
- C. 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.

- 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.

[Check answer to Question #299](#)

Question #300

A digital media company shares static content to its premium users around the world and 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. Amazon CloudFront
- C. AWS Lambda
- D. AWS Global Accelerator
- E. AWS Fargate

[Check answer to Question #300](#)

Question #301

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 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.
 - C. 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.
 - D. 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.

[Check answer to Question #301](#)

Question #302

You have a cryptocurrency exchange portal which is hosted in an Auto Scaling group of EC2 instances behind an Application Load Balancer and are deployed across multiple AWS regions. Your 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 your Japanese users to connect to the servers in the ap-northeast-1 Asia Pacific (Tokyo) region, while your Swedish users should be connected to the servers in the eu-west-1 EU (Ireland) region.

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

- A. Use Route 53 Geolocation Routing policy.
- B. Use Route 53 Weighted Routing policy.
- C. Set up an Application Load Balancers that will automatically route the traffic to the proper AWS region.
- D. Set up a new CloudFront web distribution with the geo-restriction feature enabled.

[Check answer to Question #302](#)

Question #303

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

[Check answer to Question #303](#)

Question #304

You are helping a new DevOps Engineer to design her first architecture in AWS. She is planning to develop a highly available and fault-tolerant architecture which 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 which 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 you should recommend for her to use?

- A. Either a Classic Load Balancer or a Network Load Balancer
- B. Network Load Balancer
- C. Classic Load Balancer

D. Application Load Balancer

[Check answer to Question #304](#)

Question #305

You are developing a meal planning application that provides meal recommendations for the week as well as the food consumption of your users. Your 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 your EC2 instance to access your 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 the EC2 instance.
- C. Create a role in IAM and assign it to the EC2 instance.
- D. Store the API credentials in a bastion host.

[Check answer to Question #305](#)

Question #306

To protect your enterprise applications against unauthorized access, you configured multiple rules for your Network ACLs in your VPC.

How are the access rules evaluated?

- A. Network ACL Rules are evaluated by rule number, from highest to lowest and are executed immediately when a matching allow/deny rule is found.
- B. By default, all Network ACL Rules are evaluated before any traffic is allowed or denied.
- C. Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found.

- D. Network ACL Rules are evaluated by rule number, from lowest to highest, and executed after all rules are checked for conflicting allow/deny rules.

[Check answer to Question #306](#)

Question #307

You are working for a litigation firm as the Data Engineer for their case history application. You need to keep track of all the cases your 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 your business, you want to keep track of what's happening in your S3 bucket. You 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. SES
- B. Lambda function
- C. SWF
- D. SQS
- E. Kinesis

[Check answer to Question #307](#)

Question #308

The operations team of your company asked you for a way to monitor the health of your production EC2 instances in AWS. You told them to use the CloudWatch service.

Which of the following metrics is not available by default in CloudWatch?

- A. CPU Usage
- B. Memory Usage

- C. Network In and Out
- D. Disk Read operations

[Check answer to Question #308](#)

Question #309

A company has an enterprise web application hosted in an AWS Fargate cluster with 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 if the primary application stack experiences an outage.

What should the Architect do to satisfy this requirement?

- A. 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.
- 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 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.
- D. 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.

[Check answer to Question #309](#)

Question #310

You are working for an online hotel booking firm with terabytes of customer data coming from your websites and applications. There is an annual corporate meeting where you need to present the booking behavior and acquire new insights from your customers data. You are looking for a service to perform super-fast analytics on massive data sets in near real-time.

Which of the following services gives you the ability to store huge amounts of data and perform quick and flexible queries on it?

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

[Check answer to Question #310](#)

Question #311

You run a website which accepts high-quality photos and turns them into a downloadable video montage. The website offers a free account 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 which generate the videos. You need to ensure that the premium users who paid for the service have higher priority than your free members.

How do you re-design your architecture to address this requirement?

- A. 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.
- B. Use Amazon S3 to store and process the photos and then generate the video montage afterwards.
- C. Use Amazon Kinesis to process the photos and generate the video montage in real time.
- D. 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.

[Check answer to Question #311](#)

Question #312

You are an IT Consultant for an advertising company that is currently working on a proof of concept project that automatically provides SEO analytics for their clients. Your company has a VPC in AWS that operates in 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 (techrad.io) 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 of MX record set
- E. Alias with a type "CNAME" record set

[Check answer to Question #312](#)

Question #313

An online events registration system is hosted in AWS and uses ECS to host its front-end tier and a Multi-AZ RDS for its database tier, which also has a standby replica.

What are the events that will make Amazon RDS automatically perform a failover to the standby replica? (Select TWO.)

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

[Check answer to Question #313](#)

Question #314

A startup company has a serverless architecture that uses AWS Lambda, API Gateway, and DynamoDB. They received an urgent feature request from their client last month and now, it is ready to be pushed to production. The company is using AWS CodeDeploy as their deployment service.

Which of the following configuration types will allow you to specify the percentage of traffic shifted to your updated Lambda function version before the remaining traffic is shifted in the second increment?

- A. All-at-once
- B. Canary
- C. Blue/Green
- D. Linear

[Check answer to Question #314](#)

Question #315

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 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 AWS ACM.
- B. Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets. Enable automatic rotation for all the credentials.
- C. 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.
- D. Store the database credentials, API keys, and other secrets in AWS KMS.

[Check answer to Question #315](#)

Question #316

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. Create CloudWatch alarms that stop and start the instance based on status check alarms.
- B. Write a python script that queries the EC2 API for each instance status check
- C. Buy and implement a third-party monitoring tool.

- D. Write a shell script that periodically shuts down and starts instances based on certain stats.

[Check answer to Question #316](#)

Question #317

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. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- B. Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.
- C. Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- D. Establish a hardware VPN over the Internet between VPC-1 and the on-premises network.
- E. Establish another AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1.

[Check answer to Question #317](#)

Question #318

You have two On-Demand EC2 instances inside your 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 want to ensure that these two instances can communicate with each other for your system to work properly.

What are the things you must check so that these EC2 instances can communicate inside the VPC? (Select TWO.)

- A. Check if both instances are the same instance class.
- B. Ensure that the EC2 instances are in the same Placement Group.
- C. Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.
- 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.

[Check answer to Question #318](#)

Question #319

A corporate and investment bank has recently decided to adopt a hybrid cloud architecture for their Trade Finance web application which uses an Oracle database with Oracle Real Application Clusters (RAC) configuration. Since Oracle RAC is not supported in RDS, they decided to launch their database in a large On-Demand EC2 instance instead, with multiple EBS Volumes attached.

As a Solutions Architect, you are responsible to ensure the security, availability, scalability, and disaster recovery of the whole architecture. In this scenario, which of the following will enable you to take backups of your EBS volumes that are being used by the Oracle database?

- A. Use Disk Mirroring, which is also known as RAID 1, that replicates data to two or more disks/EBS Volumes.
- B. Launch the EBS Volumes to a Placement Group which will automatically back up your data.
- C. Create snapshots of the EBS Volumes.
- D. EBS-backed EC2 instances.

[Check answer to Question #319](#)

Question #320

You are working as a Solutions Architect for an investment bank and your Chief Technical Officer intends to migrate all your applications to AWS. You are looking for block storage to store all your data and have decided to go with EBS volumes. Your boss is worried that EBS volumes are not appropriate for your 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 your migration? (Select TWO.)

- A. 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.
- B. EBS volumes can be attached to any EC2 Instance in any Availability Zone.
- C. 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
- 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. An EBS volume is off-instance storage that can persist independently from the life of an instance.

[Check answer to Question #320](#)

Question #321

As a Network Architect developing a food ordering application, you need to retrieve the instance ID, public keys, and public IP address of the EC2 server you made for tagging and grouping the attributes into your internal application running on-premises.

Which EC2 feature will help you achieve your requirements?

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

[Check answer to Question #321](#)

Question #322

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

[Check answer to Question #322](#)

Question #323

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. Use Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application.

- B. Block all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List.
- 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. 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.

[Check answer to Question #323](#)

Question #324

You are an AWS Network Engineer working for a utility provider where you are managing a monolithic application with an EC2 instance using a Windows AMI. The legacy application must maintain the same private IP address and MAC address for it to work.

You want to implement a cost-effective and highly available architecture for your application by launching a standby EC2 instance that is an exact replica of the Windows server. If the primary instance terminates, you can attach the ENI to the standby secondary instance, which allows the traffic flow to resume within a few seconds.

When it comes to the ENI attachment to an EC2 instance, what does 'warm attach' refer to?

- A. Attaching an ENI to an instance when it is running.
- B. Attaching an ENI to an instance during the launch process.
- C. Attaching an ENI to an instance when it is idle.
- D. Attaching an ENI to an instance when it is stopped.

[Check answer to Question #324](#)

Question #325

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 report 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 multiple EC2 instance stores for data storage and ElastiCache as the CDN.
- D. Use Amazon Glacier as the data storage and ElastiCache as the CDN.

[Check answer to Question #325](#)

Question #326

You are working as a Solutions Architect for a major telecommunications company where you are assigned to improve the security of your database tier by tightly managing the data flow of your Amazon Redshift cluster. One of the requirements is to use VPC flow logs to monitor all the COPY and UNLOAD traffic of your Redshift cluster that moves in and out of your VPC.

Which of the following is the most suitable solution to implement in this scenario?

- A. Enable Enhanced VPC routing on your Amazon Redshift cluster.
- B. Use the Amazon Redshift Spectrum feature.
- C. Create a new flow log that tracks the traffic of your Amazon Redshift cluster.
- D. Enable Audit Logging in your Amazon Redshift cluster.

[Check answer to Question #326](#)

Question #327

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

[Check answer to Question #327](#)

Question #328

In the VPC that you are managing, it has one EC2 instance that has its data stored in an instance store. The instance was shut down by a 2nd level support staff over the weekend to save costs. When you arrived in the office the next Monday, you noticed that all data are lost and are no longer available on the EC2 instance. What might be the cause of this?

- A. The EC2 instance was using an instance store hence, data will be erased when the instance is stopped or terminated.
- B. The EC2 instance was using EBS-backed root volumes hence, the data will be erased when the instance is shut down or stopped.
- C. The EC2 instance has been hacked.
- D. AWS automatically erased the data due to a virus found on the EC2 instance.

[Check answer to Question #328](#)

Question #329

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

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

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

[Check answer to Question #329](#)

Question #330

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

[Check answer to Question #330](#)

Question #331

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

[Check answer to Question #331](#)

Question #332

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 KMS-managed customer master key.
- B. Use S3 server-side encryption with a KMS managed key.
- C. Use S3 server-side encryption with customer provided key.
- D. Use S3 client-side encryption with a client-side master key.

[Check answer to Question #332](#)

Question #333

You are working for a software company that has moved a legacy application from an on-premises data center to the cloud. The legacy application requires a static IP address hard-coded into the backend, which blocks you from using an Application Load Balancer.

Which steps would you take to apply high availability and fault tolerance to this application without ELB? (Select TWO.)

- A. Assign an Elastic IP address to the instance.
- B. Write a script that checks the health of the EC2 instance. If the instance stops responding, the script will switch the elastic IP address to a standby EC2 instance.
- C. Launch the instance using Auto Scaling which will deploy the instance again if it becomes unhealthy.
- D. Use Cloudfront with a custom origin pointed to your on-premises network where the web application is deployed.
- E. Postpone the deployment until you have fully converted the application to work with the ELB and Auto Scaling.

[Check answer to Question #333](#)

Question #334

You are designing a banking portal which 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 must 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. 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.

- B. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.
- C. Set up a Redis replication group and enable the AtRestEncryptionEnabled parameter.
- D. Enable the in-transit encryption for Redis replication groups.

[Check answer to Question #334](#)

Question #335

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 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 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.
- B. Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and 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.
- C. Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and 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 CloudWatch trail in a new S3 bucket using the CloudTrail console and 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.

[Check answer to Question #335](#)

Question #336

You have a new joiner in your organization. You have provisioned an IAM user for the new employee in AWS however, the user is not able to perform any actions.

What could be the reason for this?

- A. IAM users are created by default with partial permissions
- B. You need to wait for 24 hours for the new IAM user to have access.
- C. IAM users are created by default with no permissions
- D. IAM users are created by default with full permissions

[Check answer to Question #336](#)

Question #337

A traffic monitoring and reporting application uses Kinesis to accept real-time data. In order to process and store the data, they used Amazon Kinesis Data Firehose to load the streaming data to various AWS resources.

Which of the following services can you load streaming data into?

- A. Amazon Redshift Spectrum

- B. Amazon Elasticsearch Service
- C. Amazon Athena
- D. Amazon S3 Select

[Check answer to Question #337](#)

Question #338

You are working for a large financial company as an IT consultant. Your role is to help their development team to 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. Redshift Spectrum
- B. ElastiCache
- C. Glacier
- D. DynamoDB
- E. RDS

[Check answer to Question #338](#)

Question #339

You are working as a Solutions Architect in a new startup that provides storage for high-quality photos which are infrequently accessed by the users. To make the architecture cost-effective, you designed the cloud service to use an S3 One Zone-Infrequent Access (S3 One Zone-IA) storage type for free users and an S3 Standard-Infrequent Access (S3 Standard-IA) storage type for premium users.

When your manager found out about this, he asked you about the differences between using S3 One Zone-IA and S3 Standard-IA. What will you say to your manager? (Select TWO.)

- A. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ.

- B. S3 One Zone-IA offers lower durability and low throughput compared with Amazon S3 Standard and S3 Standard-IA which is why it has a low per GB storage price and per GB retrieval fee.
- C. Storing data in S3 One Zone-IA costs more than storing it in S3 Standard-IA but provides more durability.
- D. Storing data in S3 One Zone-IA costs less than storing it in S3 Standard-IA.
- E. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in two AZs only. Hence the name, One Zone-IA since the data replication is skipped in one Availability Zone.

[Check answer to Question #339](#)

Question #340

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. 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.

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

[Check answer to Question #340](#)

Question #341

You are leading a software development team which uses serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. You 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 your application. You instructed one of your junior developers 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 you secure this information to prevent other developers in your team, or anyone, from seeing these credentials in plain text? Select the best option that provides the maximum security.

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

[Check answer to Question #341](#)

Question #342

A Solutions Architect is tasked to host a web application in a new VPC with private and public subnets. In order to do this, the Architect will need to deploy a new MySQL database server and a fleet of EC2 instances to host the application. In which subnet should the Architect launch the new database server into?

- A. The private subnet
- B. The public subnet
- C. Ideally be launched outside the Amazon VPC
- D. Either public or private subnet

[Check answer to Question #342](#)

Question #343

You are managing a suite of applications in your on-premises network which are using trusted IP addresses that your partners and customers have whitelisted in their firewalls. There is a requirement to migrate these applications to AWS without requiring your partners and customers to change their IP address whitelists.

Which of the following is the most suitable solution to properly migrate your applications?

- A. Set up an IP match condition using a CloudFront web distribution and AWS WAF to whitelist a specific IP address range in your VPC.
- B. Set up a list of Elastic IP addresses to map the whitelisted IP address range in your on-premises network.
- C. Create a Route Origin Authorization (ROA) then once done, provision and advertise your whitelisted IP address range to your AWS account.
- D. Submit an AWS Request Form to migrate the IP address range that you own to your AWS Account.

[Check answer to Question #343](#)

Question #344

A leading utilities provider is in the process of migrating their applications to AWS. Their Solutions Architect created an EBS-Backed EC2 instance with ephemeral0 and ephemeral1 instance store volumes attached to host a web application that fetches and stores data from a web API service. If this instance is stopped, what will happen to the data on the ephemeral store volumes?

- A. Data is unavailable until the instance is restarted.
- B. Data is automatically saved as an EBS snapshot.
- C. Data is automatically saved in an EBS volume.
- D. Data will be deleted.

[Check answer to Question #344](#)

Question #345

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. Consolidate all the company's accounts using AWS ParallelCluster.
- B. Use AWS Control Tower to easily and securely share your resources with your AWS accounts.
- C. Use the AWS Resource Access Manager (RAM) service to easily and securely share your resources with your AWS accounts.
- D. Consolidate all the company's accounts using AWS Organizations.

- E. 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.

[Check answer to Question #345](#)

Question #346

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

[Check answer to Question #346](#)

Question #347

You are a Solutions Architect in your company working with 3 DevOps Engineers under you. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service. What can you do to prevent this from happening again?

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

[Check answer to Question #347](#)

Question #348

A company has an On-Demand EC2 instance that is transferring large amounts of data to an Amazon S3 bucket in the same region. Your manager is worried about infrastructure cost considering the vast amounts of data being transferred to the bucket. What will you say to justify this architecture?

- A. Transferring data from an EC2 instance to an S3 bucket in the same region has no cost at all.
- B. Transferring data from an EC2 instance to an S3 bucket in the same region has a 50% discount based on the AWS Pricing.
- C. You are only using an On-Demand EC2 instance so the cost will be lower than a Spot instance.
- D. You are only using an On-Demand EC2 instance which is exactly the same price as Spot EC2 instance, launched by a persistent Spot request.

[Check answer to Question #348](#)

Question #349

You have launched a new enterprise application with a web server and a database. You are using a large EC2 Instance with one 500 GB EBS volume to host a relational database. Upon checking the performance, it shows that write throughput to the database needs to be improved.

Which of the following is the most suitable configuration to help you achieve this requirement? (Select TWO.)

- A. Set up a standard RAID 0 configuration with two EBS Volumes
- B. Use a standard RAID 1 configuration with two EBS Volumes
- C. Re-launch the instance with a Paravirtual (PV) AMI and enable Enhanced Networking
- D. Increase the size of the EC2 Instance
- E. Set up the EC2 instance in a placement group

[Check answer to Question #349](#)

Question #350

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

[Check answer to Question #350](#)

Question #351

A Solutions Architect is hosting a website in an Amazon S3 bucket named techradio. The users load the website using the following URL:
<http://techradio.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 (techradio.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-origin resource sharing (CORS) configuration in the bucket.
- B. Enable Cross-Region Replication (CRR).
- C. Enable cross-account access.
- D. Enable Cross-Zone Load Balancing.

[Check answer to Question #351](#)

Question #352

A startup based in Australia is deploying a new two-tier web application in AWS. The Australian company wants to store their most frequently used data in an in-memory data store to improve the retrieval and response time of their web application. Which of the following is the most suitable service to be used for this requirement?

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

[Check answer to Question #352](#)

Question #353

You founded a tech startup that provides online training and software development courses to various students across the globe. Your team has developed an online portal in AWS where the students can log into and access the courses they are subscribed to.

Since you are in the early phases of the startup and the funding is still hard to come by, which service can help you manage the budgets for all your AWS resources?

- A. Payment History
- B. Cost Allocation Tags
- C. AWS Budgets

D. Cost Explorer

[Check answer to Question #353](#)

Question #354

You are an AWS Solutions Architect designing an online analytics application that uses Redshift Cluster for its data warehouse. Which service will allow you to monitor all API calls to your Redshift instance and can also provide secured data for auditing and compliance purposes?

- A. AWS X-Ray
- B. CloudTrail for security logs
- C. CloudWatch
- D. Redshift Spectrum

[Check answer to Question #354](#)

Question #355

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 an effective method to mitigate this issue?

- A. Use CloudFront distributions for your photos.
- B. Store photos on an Amazon EBS volume of the web server.
- C. Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.
- D. Block the IP addresses of the offending websites using NACL.

[Check answer to Question #355](#)

Question #356

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

[Check answer to Question #356](#)

Question #357

You are building a new 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 high-throughput 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. Cold HDD (sc1)
- B. Throughput Optimized HDD (st1)
- C. Provisioned IOPS SSD (io1)
- D. General Purpose SSD (gp2)

[Check answer to Question #357](#)

Question #358

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

[Check answer to Question #358](#)

Question #359

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. Enabled Multi-AZ failover
- D. Create a read replica

[Check answer to Question #359](#)

Question #360

In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances. Which of the following IPv4 CIDR block can you use for this scenario?

- A. 172.0.0.0/27

- B. 172.0.0.0/29
- C. 172.0.0.0/30
- D. 172.0.0.0/28

[Check answer to Question #360](#)

Question #361

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. 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.
- C. 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.
- 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.

[Check answer to Question #361](#)

Question #362

You have a new e-commerce web application written in Angular framework which is deployed to a fleet of EC2 instances behind an Application Load Balancer. You configured the load balancer to perform health checks on these EC2 instances. What will happen if one of these EC2 instances failed the health checks?

- A. The EC2 instance is replaced automatically by the Application Load Balancer.
- B. The EC2 instance gets terminated automatically by the Application Load Balancer.
- C. The EC2 instance gets quarantined by the Application Load Balancer for root cause analysis.
- D. The Application Load Balancer stops sending traffic to the instance that failed its health check.

[Check answer to Question #362](#)

Question #363

A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances which use Amazon Aurora as its database. Currently, the system stores the file documents that the users uploaded 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 throughput POSIX-compliant file system?

- A. Use EFS
- B. Upgrade your existing EBS volumes to Provisioned IOPS SSD Volumes
- C. Use ElastiCache
- D. Create an S3 bucket and use this as the storage for the CMS

[Check answer to Question #363](#)

Question #364

There are many clients complaining that the online trading application of an investment bank is always down. Your manager instructed you to redesign the architecture of the application to prevent the unnecessary service interruptions. To ensure high availability, you set up the application to use an ELB to distribute the incoming requests across an auto-scaled group of EC2 instances in two single Availability Zones.

The Auto Scaling group is configured with default settings. In this scenario, what happens when an EC2 instance behind an ELB fails a health check?

- A. The EC2 instance gets terminated automatically by the ELB.
- B. The EC2 instance is replaced automatically by the ELB.
- C. The ELB stops sending traffic to the EC2 instance
- D. The EC2 instance will automatically be deregistered from the default Placement Group.

[Check answer to Question #364](#)

Question #365

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 several 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. 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.

- C. 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.
- 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. 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.

[Check answer to Question #365](#)

Question #366

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 user and be notified via email. Which of the following is the most suitable solution that you should implement to meet the requirement?

- A. 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.
- 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. 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 user.

- D. 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 user, notify the subscribers via email using SNS.

[Check answer to Question #366](#)

Question #367

Your company announced that there would be a surprise IT audit on all 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 Scheduled Reserved EC2 instances in your applications. They argued that you should have used Spot EC2 instances instead as it is cheaper than the Reserved Instance.

Which of the following are the characteristics and benefits of using these two types of Reserved EC2 instances, which you can use as justification? (Select TWO.)

- A. Reserved Instances doesn't get interrupted unlike Spot instances if there are not enough unused EC2 instances to meet the demand.
- B. It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration.
- C. Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances
- D. You can have capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term through Scheduled Reserved Instances
- E. It runs in a VPC on hardware that's dedicated to a single customer.

[Check answer to Question #367](#)

Question #368

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 storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates 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. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.
- B. Set up a Federation proxy or an Identity provider and use AWS Security Token Service to generate temporary tokens.
- C. Use a resource tag on each folder in the S3 bucket.
- D. Set up a matching IAM user for each 1200 users in your corporate directory that needs access to a folder in the S3 bucket.
- E. Configure an IAM role and an IAM Policy to access the bucket.

[Check answer to Question #368](#)

Question #369

You are working as a Solutions Architect in a top software development company in Silicon Valley. The company has multiple applications hosted in their VPC. While you are monitoring the system, you noticed that multiple port scans are coming in from a specific IP address block which are trying to connect to several AWS resources inside your 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. Create a policy in IAM to deny access from the IP Address block.

- B. Configure the firewall in the operating system 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. Add a rule in the Security Group of the EC2 instances to deny access from the IP Address block.

[Check answer to Question #369](#)

Question #370

You are designing a multi-tier web application architecture that consists of a fleet of EC2 instances and an Oracle relational database server. It is required that the database is highly available and that you have full control over its underlying operating system. Which AWS service will you use for your database tier?

- A. Amazon EC2 instances with data replication between two different Availability Zones
- B. Amazon RDS
- C. Amazon EC2 instances with data replication in one Availability Zone
- D. Amazon RDS with Multi-AZ deployments

[Check answer to Question #370](#)

Question #371

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 must 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. Use a combination of IAM and STS to restrict access to your RDS instance via a temporary token.
- C. Configure SSL in your application to encrypt the database connection to RDS.
- D. Enable the IAM DB Authentication.

[Check answer to Question #371](#)

Question #372

You have identified a series of DDoS attacks while monitoring your VPC. As the Solutions Architect, you are responsible in fortifying your current cloud infrastructure to protect the data of your clients. Which of the following is the most suitable solution to mitigate these kinds of attacks?

- A. Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic.
- B. Use AWS Shield to detect and mitigate DDoS attacks.
- C. Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks and other DDoS attacks.
- D. A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC.

[Check answer to Question #372](#)

Question #373

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 metric, which is not readily available in CloudWatch. Which of the following is a custom metric in CloudWatch which you must manually set up?

- A. Network packets out of an EC2 instance
- B. Disk Reads activity of an EC2 instance
- C. Memory Utilization of an EC2 instance

D. CPU Utilization of an EC2 instance

[Check answer to Question #373](#)

Question #374

You have a requirement to make sure that an 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, Source 110.238.98.71/0
- B. Security Group Inbound Rule: Protocol TCP, Port Range 22, Source 110.238.98.71/32
- C. Security Group Inbound Rule: Protocol TCP, Port Range 22, Source 110.238.98.71/0
- D. Security Group Inbound Rule: Protocol UDP, Port Range 22, Source 110.238.98.71/32

[Check answer to Question #374](#)

Question #375

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 set for long polling, so the messages are being sent twice.
- B. The web application is not deleting the messages in the SQS queue after it has processed them.
- C. The web application is set to short polling, so some messages are not being picked up
- D. The web application does not have permission to consume messages in the SQS queue.

[Check answer to Question #375](#)

Question #376

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 implementing for your DynamoDB table?

- A. Use partition keys with low-cardinality attributes, which have a few numbers of distinct values for each item.
- B. Use partition keys with high-cardinality attributes, which have many distinct values for each item.
- C. Avoid using a composite primary key, which is composed of a partition key and a sort key.
- D. Reduce the number of partition keys in the DynamoDB table.

[Check answer to Question #376](#)

Question #377

An online cryptocurrency exchange platform is hosted in AWS which uses ECS Cluster and RDS in Multi-AZ 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 must 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. 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.
- B. Enable Enhanced Monitoring in RDS.
 - C. Use Amazon CloudWatch to monitor the CPU Utilization of your database.
 - D. 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.

[Check answer to Question #377](#)

Question #378

Your cloud architecture is composed of Linux and Windows EC2 instances which process high volumes of financial data 24 hours a day, 7 days a week. To ensure high availability of your systems, you are required to monitor the memory and disk utilization of all your instances.

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

- A. Install the CloudWatch agent to all your EC2 instances which gathers the memory and disk utilization data. View the custom metrics in the Amazon CloudWatch console.
- B. Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all your EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard.
- C. Use Amazon Inspector and install the Inspector agent to all your EC2 instances.
- D. Use the default CloudWatch configuration to your EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all your EC2 instances.

[Check answer to Question #378](#)

Question #379

You are working as a Solutions Architect for a government project in which they are building an online portal to allow people to pay their taxes and claim their tax refunds online. Due to the confidentiality of data, the security policy requires that the application hosted in EC2 encrypts the data first before writing it to the disk for storage. In this scenario, which service would you use to meet this requirement?

- A. EBS encryption
- B. Elastic File System (EFS)
- C. Security Token Service
- D. AWS KMS API

[Check answer to Question #379](#)

Question #380

You have a web application deployed in AWS which is currently running in the eu-central-1 region. You have an Auto Scaling group of On-Demand EC2 instances which are using pre-built AMIs. Your manager instructed you to implement disaster recovery for your system so if the application goes down in the eu-central-1 region, a new instance can be started in the us-west-2 region. As part of your disaster recovery plan, which of the following should you take into consideration?

- A. Copy the AMI from the eu-central-1 region to the us-west-2 region. Afterwards, create a new Auto Scaling group in the us-west-2 region to use this new AMI ID.
- B. In the AMI dashboard, add the us-west-2 region to the Network Access Control List which contains the regions that can use the AMI.
- C. None. AMIs can be used in any region hence, there is no problem using it in the us-west-2 region.
- D. Share the AMI to the us-west-2 region.

[Check answer to Question #380](#)

Question #381

A company is using Redshift for its online analytical processing (OLAP) application which processes complex queries against large datasets. There is a requirement in which you must define the number of query queues that are available and how queries are routed to those queues for processing.

Which of the following will you use to meet this requirement?

- A. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use RDS database instead.
- B. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use a NoSQL DynamoDB database instead.
- C. Create a Lambda function that can accept the number of query queues and use this value to control Redshift.
- D. Use the workload management (WLM) in the parameter group configuration.

[Check answer to Question #381](#)

Question #382

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

[Check answer to Question #382](#)

Question #383

You have one security group associated with 10 On-Demand EC2 instances. You then modified the security group to allow all inbound SSH traffic and then right after that, you created two new EC2 instances in the same security group. When will the changes be applied to the EC2 instances?

- A. Immediately to all 12 instances in the security group.
- B. Immediately to the new instances, but not for the old ones which must be restarted before the changes take effect.
- C. Immediately to the new instances only.
- D. The changes will apply to all 12 instances after an hour when the propagation is complete.

[Check answer to Question #383](#)

Question #384

You are working as a Solutions Architect for a technology company which is in the process of migrating their applications to AWS. One of their systems requires a database that can scale globally and can 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 low-latency response to high-traffic queries. Which is the most suitable database solution to use to achieve this requirement?

- A. Amazon DynamoDB
- B. An Amazon RDS instance in Multi-AZ Deployments configuration
- C. An Amazon Aurora database with Read Replicas
- D. Redshift

[Check answer to Question #384](#)

Question #385

You are a Solutions Architect for a leading Enterprise Resource Planning (ERP) solutions provider, and you are instructed to design and set up the architecture of your ERP application in AWS. Your manager instructed you to avoid using fully-managed AWS services and instead, only use specific services which allows you to access the underlying operating system for the resource. This is to allow the company to have a much better control of the underlying resources that their systems are using in the AWS cloud.

Which of the following services should you choose to satisfy this requirement? (Select TWO.)

- A. Amazon EC2
- B. Amazon Athena
- C. DynamoDB
- D. Amazon Neptune
- E. Amazon EMR

[Check answer to Question #385](#)

Question #386

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 must 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. 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 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.

- B. 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.
- 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.
- D. 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 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 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.

[Check answer to Question #386](#)

Question #387

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 DynamoDB Accelerator (DAX)
- C. AWS Device Farm
- D. Amazon ElastiCache

[Check answer to Question #387](#)

Question #388

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. Launch an Oracle database instance in RDS with Recovery Manager (RMAN) enabled.
- B. Launch an Oracle Real Application Clusters (RAC) in RDS.
- C. Create an Oracle database in RDS with Multi-AZ deployments.
- D. Migrate your Oracle data to Amazon Aurora by converting the database schema using AWS Schema Conversion Tool and AWS Database Migration Service.

[Check answer to Question #388](#)

Question #389

A pharmaceutical company has resources hosted on both their on-premises network and in AWS cloud. They want all 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. Use Amazon VPC
- B. Use IAM users
- C. Set up SAML 2.0-Based Federation by using a Web Identity Federation.
- D. Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS).

[Check answer to Question #389](#)

Question #390

You have triggered the creation of a snapshot of your EBS volume attached to an Instance Store-backed EC2 Instance and is currently on-going. At this point, what are the things that the EBS volume can or cannot do?

- A. The volume can be used in write-only mode while the snapshot is in progress.
- B. The volume can be used as normal while the snapshot is in progress.
- C. The volume cannot be used until the snapshot completes.
- D. The volume can be used in read-only mode while the snapshot is in progress.

[Check answer to Question #390](#)

Question #391

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. EFS
- B. EBS
- C. S3
- D. Glacier

[Check answer to Question #391](#)

Question #392

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 host conditions to define rules that forward requests to different target groups based on the host name in the host header. This enables you to support multiple domains using a single load balancer.
- B. Replace your ALB with a Classic 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 path conditions to define rules that forward requests to different target groups based on the URL in the request.
- 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.

[Check answer to Question #392](#)

Question #393

A leading telecommunications company wants to create standard templates of their infrastructure for AWS deployment. Which AWS service can be used in this scenario?

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

[Check answer to Question #393](#)

Question #394

A media company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use a fleet of EC2 instances that pull transcoding jobs from SQS. Why is SQS an appropriate service for this scenario?

- A. SQS guarantees the order of the messages.
- B. SQS synchronously provides transcoding output.
- C. SQS checks the health of the worker instances.
- D. SQS helps to facilitate horizontal scaling of encoding tasks.

[Check answer to Question #394](#)

Question #395

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? (Choose 2)

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

[Check answer to Question #395](#)

Question #396

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. VPC Flow Logs
- B. CloudWatch
- C. CloudTrail
- D. AWS X-Ray

[Check answer to Question #396](#)

Question #397

A start-up company that offers an automated transcription service has consulted you about their AWS architecture. They have a fleet of Amazon EC2 worker instances that process an uploaded audio file and then generate a text file as an output. You must store both uploaded audio and

generated text file in the same durable storage until the user has downloaded them. The number of files to be stored can grow over time as the start-up company is expanding rapidly overseas.

Which of the following storage option should you use for this scenario, which is both cost-efficient and scalable?

- A. Amazon Redshift
- B. Amazon Glacier
- C. Amazon S3
- D. Multiple instance stores

[Check answer to Question #397](#)

Question #398

A tech company is currently using Amazon Simple Workflow (SWF) service with a default configuration for their order processing system. The system works fine but you noticed that some of the orders seem to be stuck for almost 4 weeks. What could be the possible reason for this?

- A. It is because SWF is waiting human input from an activity task.
- B. The workflow has exceeded SWFs 15-day maximum workflow execution time.
- C. The workflow has exceeded SWFs 14-day maximum workflow execution time.
- D. SWF should be restarted.

[Check answer to Question #398](#)

Question #399

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 not using a Multi-AZ RDS deployment for the development and test database
- C. Consider using Spot instances instead of reserved EC2 instances
- D. Consider removing the Elastic Load Balancer

[Check answer to Question #399](#)

Question #400

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 username and password. How can you implement this in AWS?

- A. Add multi-factor authentication (MFA) to a user pool in Cognito to protect the identity of your users.
- B. Add a new IAM policy to a user pool in Cognito.
- C. Integrate Cognito with Amazon SNS Mobile Push to allow additional authentication via SMS.
- D. Develop a custom application that integrates with Cognito that implements a second layer of authentication.

[Check answer to Question #400](#)

Question #401

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. Create Amazon Aurora Replicas.
- B. Deploy Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing.
- C. Enable Hash Joins to improve the database query performance.
- D. Use an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes.

[Check answer to Question #401](#)

Question #402

A web application that you developed stores sensitive information on a non-boot, unencrypted Amazon EBS data volume attached to an Amazon EC2 instance. Which of the following ways could provide protection to the sensitive data of your Amazon EBS volume?

- A. Create a new snapshot of the current Amazon EBS volume. Restore the snapshot to a new, encrypted Amazon EBS volume. Mount the Amazon EBS volume.
- B. Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume and finally, delete the old Amazon EBS volume.
- C. Unmount the EBS volume and then set the encryption attribute to true. Afterwards, re-mount the Amazon EBS volume to the instance.

- D. Associate the Amazon EBS volume with your AWS CloudHSM and then remount the Amazon EBS volume.

[Check answer to Question #402](#)

Question #403

You are working as the Solutions Architect for a global technology consultancy firm which 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). Your manager instructed you to set up a latency-based routing to route incoming traffic for www.techrad.io 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 Route 53 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. This is not possible in AWS. You can only set up a latency-based routing in one AWS region.

[Check answer to Question #403](#)

Question #404

An AWS account has an ID of 0499802888. Which of the following URLs would you provide to the IAM user to be able to access the AWS Console?

- A. <https://0499802888.signin.aws.amazon.com/console>
- B. <https://signin.0499802888.aws.amazon.com/console>
- C. <https://signin.aws.amazon.com/console>
- D. <https://aws.amazon.com/console>

[Check answer to Question #404](#)

Question #405

For data privacy, a healthcare company has been asked to comply with the Health Insurance Portability and Accountability Act (HIPAA). They have been told that all the data being backed up or stored on Amazon S3 must be encrypted. What is the best option to do this? (Choose 2)

- 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. Store the data in encrypted EBS snapshots.
- D. Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption.
- E. Enable Server-Side Encryption on an S3 bucket to make use of AES-128 encryption.

[Check answer to Question #405](#)

Question #406

For the user session management of your web application, you are tasked to implement a technical solution to consistently route the user's request to the same EC2 instance using sticky sessions. What are the two requirements to configure sticky sessions for your Classic Load Balancer?

- A. An HTTP/HTTPS load balancer and at least one healthy instance in each Availability Zone.
- B. A Network Load Balancer and at least one healthy instance in each Availability Zone.
- C. An HTTP/HTTPS load balancer and EC2 instance with a RAID volume
- D. A Network Load Balancer and at least two healthy instances in each Availability Zone.

[Check answer to Question #406](#)

Question #407

You are working for a litigation firm as the Data Engineer for their case history application. You need to keep track of all the cases your 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 your business, you want to keep track of what's happening in your S3 bucket. You 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? (Choose 2)

- A. Kinesis
- B. SES
- C. SQS
- D. Lambda function
- E. SWF

[Check answer to Question #407](#)

Question #408

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? (Choose 2)

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

[Check answer to Question #408](#)

Question #409

A data analytics application requires a service that can collect, process, and analyze clickstream data from various websites in real-time. Which of the following is the most suitable service to use for the application?

- A. Kinesis
- B. Redshift Spectrum
- C. AWS Glue
- D. Amazon EMR

[Check answer to Question #409](#)

Question #410

The company that you are working for has instructed you to create a cost-effective cloud solution for their online movie ticketing service. Your team has designed a solution of using a fleet of Spot EC2 instances to host the new ticketing web application.

You requested a spot instance at a maximum price of \$0.06/hr which has been fulfilled immediately. After 45 minutes, the spot price increased to \$0.08/hr and then your instance was terminated by AWS.

What was the total EC2 compute cost of running your spot instances?

- A. \$0.00
- B. \$0.06
- C. \$0.08
- D. \$0.07

[Check answer to Question #410](#)

Question #411

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 metric, which is not readily available in CloudWatch. Which of the following is a custom metric in CloudWatch which you must manually set up?

- A. Memory Utilization of an EC2 instance
- B. CPU Utilization of an EC2 instance
- C. Disk Reads activity of an EC2 instance
- D. Network packets out of an EC2 instance

[Check answer to Question #411](#)

Question #412

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 CloudHSM and KMS?

- A. No major difference. They both do the same thing.
- B. AWS CloudHSM does not support the processing, storage, and transmission of credit card data by a merchant or service provider, as it has not been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS); hence, you will need to use KMS.
- C. You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.
- D. AWS CloudHSM should always be used for any payment transactions.

[Check answer to Question #412](#)

Question #413

As a Junior Software Engineer, you are developing a hotel reservations application and are given the task of improving the database aspect of the app. You found out that RDS does not satisfy the needs of your application

because it does not scale as easily compared with DynamoDB. You need to demonstrate to your Senior Software Engineer the advantages of using DynamoDB over RDS. What are the valid use cases for Amazon DynamoDB? (Choose 2)

- A. Running relational SQL joins and complex data updates.
- B. Managing web sessions.
- C. Storing large amounts of infrequently accessed data.
- D. Storing metadata for Amazon S3 objects.
- E. Storing BLOB data.

[Check answer to Question #413](#)

Question #414

You are working for a tech company which currently has an on-premise infrastructure. They are currently running low on storage and want to have the ability to extend their storage using AWS cloud. Which AWS service can help you achieve this requirement?

- A. Amazon EC2
- B. Amazon Storage Gateway
- C. Amazon Storage devices
- D. Amazon SQS

[Check answer to Question #414](#)

Question #415

You are working for an online hotel booking firm with terabytes of customer data coming from your websites and applications. There is an annual corporate meeting where you need to present the booking behavior and acquire new insights from your customers data. You are looking for a service to perform super-fast analytics on massive data sets in near real-time.

Which of the following services gives you the ability to store huge amounts of data and perform quick and flexible queries on it?

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

[Check answer to Question #415](#)

Question #416

Your IT Director instructed you to ensure that all the AWS resources in your VPC don't go beyond their service limit. Which of the following services can help in this task?

- A. AWS CloudWatch
- B. AWS EC2
- C. AWS Trusted Advisor
- D. AWS SNS

[Check answer to Question #416](#)

Question #417

You are a Solutions Architect of a media company and you are instructed to migrate an on-premise web application architecture to AWS. During your design process, you must give consideration to current on-premise security and determine which security attributes you are responsible for on AWS. Which of the following does AWS provide for you as part of the shared responsibility model?

- A. Customer Data
- B. Physical network infrastructure
- C. Instance security
- D. User access to the AWS environment

[Check answer to Question #417](#)

Question #418

You are working as a Solutions Architect in a well-funded financial startup. The CTO instructed you to launch a cryptocurrency mining server on a Reserved EC2 instance in us-east-1 region which is using IPv6. Due to the financial data the server contains, the system should be secured to avoid 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. NAT Gateway
- B. NAT instances
- C. Egress-only Internet gateway
- D. Internet Gateway

[Check answer to Question #418](#)

Question #419

A corporate and investment bank has recently decided to adopt a hybrid cloud architecture for their Trade Finance web application which uses an Oracle database with Oracle Real Application Clusters (RAC) configuration. Since Oracle RAC is not supported in RDS, they decided to launch their database in a large On-Demand EC2 instance instead, with multiple EBS Volumes attached. As a Solutions Architect, you are responsible to ensure the security, availability, scalability, and disaster recovery of the whole architecture. In this scenario, which of the following will enable you to take backups of your EBS volumes that are being used by the Oracle database?

- A. EBS-backed EC2 instances.
- B. Use Disk Mirroring, which is also known as RAID 1, that replicates data to two or more disks/EBS Volumes.
- C. Launch the EBS Volumes to a Placement Group which will automatically back up your data.
- D. Create snapshots of the EBS Volumes.

[Check answer to Question #419](#)

Question #420

You are working as a Cloud Consultant for a government agency with a mandate of improving traffic planning, maintenance of roadways and preventing accidents. There is a need to manage 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 said devices to your cloud-based applications?

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

[Check answer to Question #420](#)

Question #421

Your manager has asked you 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 into a highly scalable and highly available data store for real-time public tabulation.

Which is the best service that you should use for this scenario?

- A. Amazon DynamoDB
- B. Amazon Redshift
- C. Amazon Relational Database Service (RDS)
- D. Amazon Aurora

[Check answer to Question #421](#)

Question #422

You are an AWS Network Engineer working for a utilities provider where you are managing a monolithic application with EC2 instance using a Windows AMI. You want to implement a cost-effective and highly available architecture for your application where you have an exact replica of the Windows server that is in a running state.

If the primary instance terminates, you can attach the ENI to the standby secondary instance which allows the traffic flow to resume within a few seconds.

When it comes to the ENI attachment to an EC2 instance, what does 'warm attach' refer to?

- A. Attaching an ENI to an instance when it is stopped.
- B. Attaching an ENI to an instance during the launch process.
- C. Attaching an ENI to an instance when it is running.
- D. Attaching an ENI to an instance when it is idle.

[Check answer to Question #422](#)

Question #423

A web application is hosted in an Auto Scaling group of EC2 instances deployed across multiple Availability Zones in front of 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?
(Choose 2)

- A. AWS Certificate Manager
- B. IAM certificate store
- C. A private S3 bucket with versioning enabled

- D. An S3 bucket configured with server-side encryption with customer-provided encryption keys (SSE-C)
- E. CloudFront

[Check answer to Question #423](#)

Question #424

A loan processing application is hosted in a single On-Demand EC2 instance in your VPC. To improve the scalability of your application, you must 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? (Choose 2)

- A. You must stop the instance first.
- B. You must ensure that the AMI used to launch the instance still exists.
- C. You must ensure that the AMI used to launch the instance no longer exists.
- D. The instance is launched into one of the Availability Zones defined in your Auto Scaling group.
- E. You must ensure that the instance is in a different Availability Zone as the Auto Scaling group.

[Check answer to Question #424](#)

Question #425

You are working as a Solutions Architect for a fast-growing startup which just started operations during the past 3 months. They currently have an on-premise 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 on the existing security controls in AWS but can still communicate with their on-premise network. Which set of AWS services will you use to meet these requirements?

- A. AWS Directory Services, VPN connection, and ClassicLink
- B. AWS Directory Services, VPN connection, and Amazon Workspaces
- C. AWS Directory Services, VPN connection, and AWS Identity and Access Management
- D. AWS Directory Services, VPN connection, and Amazon S3

[Check answer to Question #425](#)

Question #426

You are an AWS Solutions Architect designing an online analytics application that uses Redshift Cluster for its data warehouse. Which service will allow you to monitor all API calls to your Redshift instance and can also provide secured data for auditing and compliance purposes?

- A. CloudTrail for security logs
- B. CloudWatch
- C. AWS X-Ray
- D. Redshift Spectrum

[Check answer to Question #426](#)

Question #427

You are building a cloud infrastructure where you have EC2 instances that require access to various AWS services such as S3 and Redshift. You will also need to provision access to system administrators so they can deploy and test their changes.

Which configuration should be used to ensure that AWS Credentials like Access Keys and Secret Access Keys are secured and not compromised? (Choose 2)

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

E. Store the AWS Access Keys in ACM.

[Check answer to Question #427](#)

Question #428

You are designing a multi-tier web application architecture that consists of a fleet of EC2 instances and an Oracle relational database server. It is required that the database is highly available and that you have full control over its underlying operating system. Which AWS service will you use for your database tier?

- A. Amazon RDS
- B. Amazon RDS with Multi-AZ deployments
- C. Amazon EC2 instances with data replication in one Availability Zone
- D. Amazon EC2 instances with data replication between two different Availability Zones

[Check answer to Question #428](#)

Question #429

Your client is an insurance company that utilizes SAP HANA for their day-to-day ERP operations. Since you can't migrate this database due to customer preferences, you need to integrate it with your current AWS workload in your VPC in which you are required to establish a site-to-site VPN connection. What needs to be configured outside of the VPC for you to have a successful site-to-site VPN connection?

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

[Check answer to Question #429](#)

Question #430

You are setting up a configuration management in your existing cloud architecture where you must deploy and manage your 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 CloudFormation
- D. AWS CodeDeploy

[Check answer to Question #430](#)

Question #431

You are instructed by your manager to create a publicly accessible EC2 instance by using an Elastic IP (EIP) address and to give him 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 stopped and it has only one associated EIP.
- D. There is no cost if the instance is running and it has at least two associated EIP.

[Check answer to Question #431](#)

Question #432

You are looking for a cloud storage for your company with the lowest possible cost. The files to be stored are rarely retrieved, however, the data

retrieval time should not exceed 24 hours. What is the best storage option to use in AWS for this scenario?

- A. Amazon Glacier
- B. Amazon S3 - Reduced Redundancy Storage
- C. Amazon S3 Standard - Infrequent Access
- D. Amazon S3 Standard

[Check answer to Question #432](#)

Question #433

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 the AWS resources that they are using. In this scenario, which of the following will incur costs? (Choose 2)

- A. A running EC2 Instance
- B. A stopped EC2 Instance
- C. EBS Volumes attached to stopped EC2 Instances
- D. Using an Amazon VPC
- E. Public Data Set

[Check answer to Question #433](#)

Question #434

You work for a leading university as an AWS Infrastructure Engineer and as a professor to aspiring AWS architects. To familiarize your students with AWS, you gave them a project to host their applications to an EC2 instance. One of your students created an instance to host their online enrollment system project but is having a hard time connecting to their newly created EC2 instance. Your students have explored all the troubleshooting guides by AWS and narrowed it down to login issues. Which of the following can you use to log into an EC2 instance?

- A. Custom EC2 password

- B. EC2 Connection Strings
- C. Key Pairs
- D. Access Keys

[Check answer to Question #434](#)

Question #435

You are responsible for running a global news website hosted in a fleet of EC2 Instances. Lately, the load on the website has increased which resulted to 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? (Choose 2)

- A. Use AWS CloudFront with website as the custom origin.
- B. For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions.
- C. Use Amazon ElastiCache for the website's in-memory data store or cache.
- D. Deploy the website to all regions in different VPCs for faster processing.

[Check answer to Question #435](#)

Question #436

You are trying to establish an SSH connection to a newly created Amazon EC2 instance using the PuTTY tool. However, you are getting the following error message: Error: No supported authentication methods available.

What steps should you take to fix this issue? (Choose 2)

- A. Verify if your private key (.pem) file has been correctly converted to the format recognized by PuTTY (.ppk).
- B. Verify that your IAM user policy has permission to launch Amazon EC2 instances.

- C. Verify that you are connecting with the appropriate username for your AMI such as ec2-user for Linux AMI, centos for Centos AMI or admin for Debian AMI
- D. Verify that the Amazon EC2 Instance was launched with the proper IAM role.
- E. Verify that you have waited at least 1 hour after the EC2 instance was created before connecting via SSH.

[Check answer to Question #436](#)

Question #437

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

How can you protect your 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

[Check answer to Question #437](#)

Question #438

You are working as a Solutions Architect for a leading pharmaceutical company which has a fleet of On-Demand Linux EC2 instances in AWS. To properly monitor your systems, you are writing a custom script which requires the MAC address, instance type, AMI ID, and other metadata of your EC2 instance.

Which of the following is the base URL that you should use to list all instance metadata?

- A. `http://254.169.169.254/latest/`
- B. `http://169.169.254.254/latest/`
- C. `http://127.0.0.1/latest/`
- D. `http://169.254.169.254/latest/`

[Check answer to Question #438](#)

Question #439

You are working as a Solutions Architect for a government project in which they are building an online portal to allow people to pay their taxes and claim their tax refunds online. Due to the confidentiality of data, the security policy requires that the application hosted in EC2 encrypts the data first before writing it to the disk for storage.

In this scenario, which service would you use to meet this requirement?

- A. Security Token Service
- B. EBS encryption
- C. Elastic File System (EFS)
- D. AWS KMS API

[Check answer to Question #439](#)

Question #440

A leading bank has an application that is hosted on an Auto Scaling group of EBS-backed EC2 instances. As the Solutions Architect, you need to provide the ability to fully restore the data stored in their EBS volumes by using EBS snapshots.

Which of the following approaches provide the lowest cost for Amazon Elastic Block Store snapshots?

- A. Maintain two snapshots: the original snapshot and the latest incremental snapshot.
- B. Maintain a volume snapshot; subsequent snapshots will overwrite one another.
- C. Just maintain a single snapshot of the EBS volume since the latest snapshot is both incremental and complete.
- D. Maintain the most current snapshot and then archive the original and incremental snapshots to Amazon Glacier.

[Check answer to Question #440](#)

Question #441

You are working as a Solutions Architect in a new startup that provides storage for high-quality photos which are infrequently accessed by the users. To make the architecture cost-effective, you designed the cloud service to use an S3 One Zone-Infrequent Access (S3 One Zone-IA) storage type for free users and an S3 Standard-Infrequent Access (S3 Standard-IA) storage type for premium users.

When your manager found out about this, he asked you about the trade-offs of using S3 One Zone-IA instead of the S3 Standard-IA. What will you say to your manager? (Choose 2)

- A. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ.
- B. Storing data in S3 One Zone-IA costs less than storing it in S3 Standard-IA.
- C. Storing data in S3 One Zone-IA costs more than storing it in S3 Standard-IA but provides more durability.
- D. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in two AZs only. Hence the name, One Zone-IA since the data replication is skipped in one Availability Zone.

- E. S3 One Zone-IA offers lower durability and low throughput compared with Amazon S3 Standard and S3 Standard-IA which is why it has a low per GB storage price and per GB retrieval fee.

[Check answer to Question #441](#)

Question #442

You are working for a large financial company as an IT consultant. Your role is to help their development team to build a highly available web application using stateless web servers. In this scenario, which AWS services are suitable for storing session state data? (Choose 2)

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

[Check answer to Question #442](#)

Question #443

You are working for a large telecommunications company. They have a requirement to move 83 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. Amazon Snowball
- B. Amazon Snowball Edge
- C. Amazon Direct Connect
- D. Amazon S3 Multi-Part Upload

[Check answer to Question #443](#)

Question #444

A global medical research company has a molecular imaging system which provides each client with frequently updated images of what is happening inside the human body at the molecular and cellular level. The system is hosted in AWS and the images are hosted in an S3 bucket behind a CloudFront web distribution.

There was a new batch of updated images that were uploaded in S3; however, the users were reporting that they were still seeing the old content. You need to control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

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

- A. Use versioned objects
- B. Invalidate the files in your CloudFront web distribution
- C. Add a separate cache behavior path for the content and configure a custom object caching with a Minimum TTL of 0
- D. Add Cache-Control no-cache, no-store, or private directives to the objects that you don't want CloudFront to cache.

[Check answer to Question #444](#)

Question #445

You have 2 SUSE Linux Enterprise Server instances located in different subnets in the same VPC. These EC2 instances should be able to communicate with each other, but you always get a timeout when you try to ping from one instance to another.

In addition, the route tables seem to be valid and have the entry for the Target local for your VPC CIDR. Which of the following could be a valid reason for this issue?

- A. The two EC2 Instances have different versions of the SUSE Linux AMI.

- B. You have not configured the Security Group to allow the required traffic between the two subnets.
- C. The EC2 instances do not have Public IPs attached to them.
- D. The EC2 Instances do not have Elastic IPs.

[Check answer to Question #445](#)

Question #446

You have a new, 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. Duplicate the exact application architecture in another region and configure DNS weight-based routing.
- B. Enable failover to an application hosted in an on-premise data center.
- C. Use Route 53 with the failover option to a static S3 website bucket or CloudFront distribution.
- D. Add more servers in case the application fails.

[Check answer to Question #446](#)

Question #447

You have designed and built a new AWS architecture. After deploying your application to an On-demand EC2 instance, you found that there is an issue in your application when connecting to port 443. After troubleshooting the issue, you added port 443 to the security group of the instance.

How long will it take before the changes are applied to all the resources in your VPC?

- A. Roughly around 5-8 minutes for the security rules to propagate.
- B. Immediately after a reboot of the EC2 instances which belong to that security group.
- C. Immediately.

- D. It takes exactly one minute for the rules to apply to all availability zones within the AWS region.

[Check answer to Question #447](#)

Question #448

You founded an artificial intelligence and machine learning startup that builds enterprise AI solutions, which can quickly turn raw data in various forms stored across siloed hardware into fully operationalized solutions, without time-consuming coding. Your cloud infrastructure is composed of auto-scaled On-Demand EC2 instances deployed to multiple Availability Zones with an ELB in front that load balances the incoming traffic.

To ensure high availability of your APIs and other services, you need to set up monitoring that checks the health of your On-Demand EC2 instances. Which of the following are best practices for monitoring your EC2 Instances?

- A. Automate monitoring tasks as much as possible.
- B. Check the log files on your EC2 instances.
- C. Make monitoring a priority to head off small problems before they become big ones.
- D. All of the above

[Check answer to Question #448](#)

Question #449

You've been instructed to create a duplicate environment in another region for your company's disaster recovery plan. Part of your environment relies on EC2 instances with pre-configured software. What step would you take to configure the instances in another region?

- A. Create an AMI of the EC2 instance
- B. Create an AMI of the EC2 instance and copy the AMI to the desired region

- C. Use IAM permissions to make the EC2 instance shareable among other regions
- D. None of the above

[Check answer to Question #449](#)

Question #450

Your company has a new online banking portal which needs to have a user session management. Which of the following can be used for session management of your application?

- A. Elastic Load Balancer, ElastiCache, and Redshift
- B. AWS Storage Gateway, ElastiCache, and Elastic Load Balancer
- C. CloudWatch, RDS, and DynamoDB
- D. ElastiCache, Amazon RDS, and DynamoDB

[Check answer to Question #450](#)

Question #451

What is the AWS Lambda resource limit for ephemeral disk capacity allocated per invocation?

- A. 1 GB
- B. 256 MB
- C. 2 GiB
- D. 512 KB
- E. 512 MB

[Check answer to Question #451](#)

Question #452

Your IT director assigned you the task of providing a single sign-on feature to all your existing users who are using on-premise web applications. How will you implement this feature?

- A. Use IAM with SAML.
- B. Use the company's LDAP directory with IAM.
- C. Use the AWS Secure Token service (STS) and SAML
- D. Use IAM and OAuth.

[Check answer to Question #452](#)

Question #453

A local bank has an in-house application which 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. Create an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3.
- B. Configure a VPC Interface Endpoint along with a corresponding route entry that directs the data to S3.
- C. Configure a VPC Endpoint Gateway along with a corresponding route entry that directs the data to S3.
- D. Provision a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3.

[Check answer to Question #453](#)

Question #454

A leading e-commerce company needs a storage solution that can be accessed by 1000 Linux servers in multiple availability zones. 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. S3
- B. EFS
- C. EBS
- D. Storage Gateway

[Check answer to Question #454](#)

Question #455

A suite of web applications is composed of several different Auto Scaling group of EC2 instances which is configured with default settings and then deployed across three Availability Zones. 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 which has the least number of user sessions
- B. The EC2 instance which has been running for the longest time
- C. The EC2 instance which belongs to an Auto Scaling group with the oldest launch configuration
- D. The instance will be randomly selected by the Auto Scaling group

[Check answer to Question #455](#)

Question #456

A financial application that calculates accruals, interests, and other data is hosted on a fleet of Spot EC2 instances that are configured with Auto Scaling. The application is used by an external reporting application that provides the total calculation for each user account and transaction. You used CloudWatch to automatically monitor the EC2 instance without manually checking the server for high CPU Utilization or crashes.

What is the time period of data that Amazon CloudWatch receives and aggregates from EC2 by default?

- A. One second
- B. Five seconds
- C. One minute
- D. Five minutes

[Check answer to Question #456](#)

Question #457

A content management system (CMS) is hosted on a fleet of auto-scaled, On-Demand EC2 instances which use Amazon Aurora as its database. Currently, the system stores the file documents that the users uploaded 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 throughput file system?

- A. Create an S3 bucket and use this as the storage for the CMS
- B. Use EFS
- C. Upgrade your existing EBS volumes to Provisioned IOPS SSD Volumes
- D. Use ElastiCache

[Check answer to Question #457](#)

Question #458

You are working for a University as their AWS Consultant. They want to have a disaster recovery strategy in AWS for mission-critical applications after suffering a disastrous outage wherein they lost student and employee records. They don't want this to happen again but at the same time want to minimize the monthly costs. You are instructed to set up a minimum version of the application that is always available in case of any outages.

Which of the following disaster recovery architectures is the most suitable one to use in this scenario?

- A. Backup & Restore
- B. Pilot Light
- C. Warm Standby
- D. Multi-Site

[Check answer to Question #458](#)

Question #459

Using the EC2 API, you requested 40 m5.large On-Demand EC2 instances in a single Availability Zone. Twenty instances were successfully created but the other 20 requests failed. What is the solution for this issue and what is the root cause?

- A. For new accounts, there is a soft limit of 20 EC2 instances per region. Submit an Amazon EC2 instance Request Form in order to lift this limit.
- B. You can only create 20 instances per Availability Zone. Select a different Availability Zone and retry creating the instances again.
- C. A certain Inbound Rule in your Network Access List is preventing you to create more than 20 instances. Remove this rule and the issue will be resolved.
- D. The API credentials that you are using has a limit of only 20 requests per hour. Try submitting the request again after one hour.

[Check answer to Question #459](#)

Question #460

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. SWF
- B. AWS Lambda
- C. AWS Step Functions
- D. AWS Batch

[Check answer to Question #460](#)

Question #461

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-premise network with VPC-1.

Which of the following options increase the fault tolerance of the connection to VPC-1? (Select all that applies.)

- 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 a hardware VPN over the Internet between VPC-1 and the on-premises network.
- C. Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.
- D. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- E. Establish another AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1.

[Check answer to Question #461](#)

Question #462

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 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? (Choose 2)

- A. By using your own keys in AWS Key Management Service (KMS).
- B. By using S3 Server-Side Encryption.
- C. By using Amazon-managed keys in AWS Key Management Service (KMS).
- D. By using S3 Client-Side Encryption.
- E. By using a password stored in CloudHSM.
- F. By using the SSL certificates provided by the AWS Certificate Manager (ACM).

[Check answer to Question #462](#)

Question #463

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

[Check answer to Question #463](#)

Question #464

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

[Check answer to Question #464](#)

Question #465

An online health record system, which provides centralized health records of all citizens, has been migrated to AWS. The system is hosted in one large EBS-backed EC2 instance which hosts both its web server and database. Which of the following does not happen when you stop a running EBS-backed EC2 instance?

- A. Any Amazon EBS volume remains attached to the instance, and their data persists.
- B. In most cases, the instance is migrated to a new underlying host computer when it's restarted.
- C. Any data stored in the RAM of the underlying host computer or the instance store volumes of the host computer are gone.
- D. If it is in the EC2-Classic platform, the instance retains its associated Elastic IP addresses.

[Check answer to Question #465](#)

Question #466

You have a web application hosted in EC2 that consumes messages from an SQS queue and is integrated with SNS to send out an email to you once the process is complete. You received 5 orders but after a few hours, you saw more than 20 email notifications in your inbox. Which of the following could be the possible culprit for this issue?

- A. The web application is set for long polling, so the messages are being sent twice.
- B. The web application is not deleting the messages in the SQS queue after it has processed them.
- C. The web application is set to short polling, so some messages are not being picked up
- D. The web application does not have permission to consume messages in the SQS queue.

[Check answer to Question #466](#)

Question #467

You are setting up a cost-effective architecture for a log processing application which has frequently accessed, throughput-intensive workloads. The application should be hosted in an On-Demand EC2 instance in your VPC.

Which of the following is the most suitable EBS volume type to use in this scenario?

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

[Check answer to Question #467](#)

Question #468

The game development company that you are working for has an Amazon VPC with a public subnet. It has 4 EC2 instances that are deployed in the public subnet. These 4 instances can successfully communicate with other hosts on the Internet. You launched a fifth instance in the same public subnet, using the same AMI and security group configuration that you used for the others.

However, this new instance cannot be accessed from the internet unlike the other instance. What should you do to enable access to the fifth instance over the Internet?

- A. Deploy a NAT instance into the public subnet.
- B. Assign an Elastic IP address to the new instance.
- C. Configure a publicly routable IP Address in the host OS of the new instance.
- D. Modify the routing table for the public subnet.

[Check answer to Question #468](#)

Question #469

You are working as a Cloud Engineer in a leading technology consulting firm which is using 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 you with 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. Egress-Only Internet Gateway
- B. VPC Endpoint
- C. NAT Gateway
- D. NAT Instance

[Check answer to Question #469](#)

Question #470

A software development company has recently invested 20 million dollars to build their own artificial intelligence APIs and AI-powered chatbots. You are hired as a Solutions Architect to build a low-cost prototype on their AWS cloud infrastructure. Which of the following combination of AWS services will provide user authentication, scalable object storage and will allow you to run your code without the need to host it in an EC2 instance?

- A. Cognito, Lambda, S3
- B. AWS IoT, Cognito, S3
- C. IAM, Lambda, EBS Volumes
- D. IAM, Cognito, EBS Volumes

[Check answer to Question #470](#)

Question #471

A startup based in Australia is deploying a new two-tier web application in AWS. The Australian company wants to store their most frequently used data in an in-memory data store to improve the retrieval and response time of their web application.

Which of the following is the most suitable service to be used for this requirement?

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

[Check answer to Question #471](#)

Question #472

There are many clients complaining that the online trading application of an investment bank is always down. Your manager instructed you to redesign the architecture of the application to prevent the unnecessary service interruptions.

To ensure high availability, you set up the application to use an ELB to distribute the incoming requests across an auto-scaled group of EC2 instances in two single Availability Zones.

In this scenario, what happens when an EC2 instance behind an ELB fails a health check?

- A. The EC2 instance gets terminated automatically by the ELB.
- B. The EC2 instance gets quarantined by the ELB for root cause analysis.
- C. The EC2 instance is replaced automatically by the ELB.
- D. The ELB stops sending traffic to the EC2 instance

[Check answer to Question #472](#)

Question #473

You are working for an advertising company as their Senior Solutions Architect handling the S3 storage data. Your company has terabytes of data sitting on AWS S3 standard storage class, which accumulates significant operational costs. The management wants to cut down on the cost of their cloud infrastructure, so you were instructed to switch to Glacier to lessen the cost per GB storage.

The Amazon Glacier storage service is primarily used for which use case? (Choose 2)

- A. Storing cached session data
- B. Storing infrequently accessed data
- C. Storing Data archives
- D. Used for active database storage
- E. Used as a data warehouse

[Check answer to Question #473](#)

Question #474

You are working for a software company that has moved a legacy application from an on-premise data center to the cloud. The legacy application requires a static IP address hard-coded into the backend, which blocks you from using an Application Load Balancer.

Which steps would you take to apply high availability and fault tolerance to this application without ELB? (Choose 2)

- A. Write a script that checks the health of the EC2 instance. If the instance stops responding, the script will switch the elastic IP address to a standby EC2 instance.
- B. Assign an Elastic IP address to the instance.
- C. Postpone the deployment until you have fully converted the application to work with the ELB and Auto Scaling.
- D. Launch the instance using Auto Scaling which will deploy the instance again if it becomes unhealthy.
- E. Use CloudFront with a custom origin pointed to your on-premise network where the web application is deployed.

[Check answer to Question #474](#)

Question #475

A traffic monitoring and reporting application uses Kinesis to accept real-time data. In order to process and store the data, they used Amazon Kinesis Data Firehose to load the streaming data to various AWS resources.

Which of the following services can you load streaming data into?

- A. Amazon S3 Select
- B. Amazon Redshift Spectrum
- C. Amazon Elasticsearch Service
- D. Amazon Athena

[Check answer to Question #475](#)

Question #476

You are leading a software development team which uses serverless computing with AWS Lambda to build and run applications without having to set up or manage servers. You have a Lambda function that connects to a MongoDB Atlas, which is a popular Database as a Service (DBaaS) platform and uses a third-party API to fetch certain data for your application.

You instructed one of your junior developers 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 you secure this information to prevent other developers in your team, or anyone, from seeing these credentials in plain text? Select the best option that provides the maximum security.

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

[Check answer to Question #476](#)

Question #477

In your AWS VPC, you need to add a new subnet that will allow you to host a total of 20 EC2 instances. Which of the following IPv4 CIDR block can you

use for this scenario?

- A. 172.0.0.0/27
- B. 172.0.0.0/28
- C. 172.0.0.0/29
- D. 172.0.0.0/30

[Check answer to Question #477](#)

Question #478

You have 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 the best to use in this case?

- A. Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.
- B. Amazon Glacier for storing the application log files and Spot EC2 Instances for processing them.
- C. A single On-Demand Amazon EC2 instance for both storing and processing the log files
- D. Amazon RedShift to store the logs and Amazon Lambda for running custom log analysis scripts

[Check answer to Question #478](#)

Question #479

Your team is planning to migrate a web application from your on-premise infrastructure to AWS cloud. Your team lead wants to ensure that even though the application will be in AWS, you can still manage the service and implement ongoing maintenance of packages. Which of the following AWS services can you use, which allows access to its underlying infrastructure? (Choose 2)

- A. Elastic Beanstalk

- B. EC2
- C. DynamoDB
- D. Amazon Athena
- E. Amazon API Gateway

[Check answer to Question #479](#)

Question #480

You are a Solutions Architect working with a company that uses Chef Configuration management in their data center. Which service is designed to let the customer leverage existing Chef recipes in AWS?

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

[Check answer to Question #480](#)

Question #481

You have a new joiner in your organization. You had provisioned an IAM user for the new employee in AWS however, the user is not able to perform any actions. What could be the reason for this?

- A. IAM users are created by default with partial permissions
- B. IAM users are created by default with full permissions
- C. IAM users are created by default with no permissions
- D. You need to wait for 24 hours for the new IAM user to have access.

[Check answer to Question #481](#)

Question #482

You have a static corporate website hosted in a standard S3 bucket and a new web domain name which 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? (Choose 2)

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

[Check answer to Question #482](#)

Question #483

You have a web application deployed in AWS which is currently running in the eu-central-1 region. You have an Auto Scaling group of On-Demand EC2 instances which are using pre-built AMIs. Your manager instructed you to implement disaster recovery for your system so if the application goes down in the eu-central-1 region, a new instance can be started in the us-west-2 region.

As part of your disaster recovery plan, which of the following should you take into consideration?

- A. In the AMI dashboard, add the us-west-2 region to the Network Access Control List which contains the regions that can use the AMI.
- B. Copy the AMI from the eu-central-1 region to the us-west-2 region. Afterwards, change the Auto Scaling groups in the us-west-2 region to use this new AMI ID.
- C. Share the AMI to the us-west-2 region.
- D. None. AMIs can be used in any region hence, there is no problem using it in the us-west-2 region.

[Check answer to Question #483](#)

Question #484

You are a Solutions Architect of a multi-national gaming company which develops video games for PS4, Xbox One and Nintendo Switch consoles, plus several mobile games for Android and iOS. Due to the wide range of their products and services, you proposed that they use API Gateway. What are the key features of API Gateway that you can tell your client? (Choose 2)

- A. It automatically provides a query language for your APIs like GraphQL.
- B. You can run your APIs with quantum computer servers.
- C. You can run your APIs without any servers.
- D. Provides durable data storage
- E. You pay only for the API calls you receive, and the amount of data transferred out.

[Check answer to Question #484](#)

Question #485

An online stock trading portal is deployed in AWS and in order to complete the set up, you need to offload the SSL/TLS processing for your web servers using CloudHSM. This will reduce the burden on your web servers and provides extra security by storing your web server's private key in this cloud-based hardware security module. Which of the following statements is not true about Amazon CloudHSM?

- A. AWS manages the hardware security module (HSM) appliance but does not have access to your keys.
- B. Your HSMs are in your Virtual Private Cloud (VPC) and isolated from other AWS networks.
- C. You control and manage your own encryption keys.
- D. It provides a secure key storage in tamper-resistant hardware available in a single Availability Zone.

[Check answer to Question #485](#)

Question #486

You want to establish an SSH connection to a Linux instance hosted in your VPC via the Internet. Which of the following is not required for this to work?

- A. Secondary Private IP Address
- B. Public IP Address or Elastic IP
- C. Internet Gateway
- D. Network access control and security group rules which allow the relevant traffic to flow to and from your EC2 instance.

[Check answer to Question #486](#)

Question #487

To save cost, a company decided to change their third-party data analytics tool to a cheaper solution. They sent a full data export on a CSV file which contains all 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 a standard SQL?

- A. 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.
- B. 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.
- C. To be able to run SQL queries, use AWS Athena to analyze the export data file in S3.
- D. Use a migration tool to load the CSV export file from S3 to a database which is designed for online analytic processing (OLAP) such as AWS

RedShift. Run some queries once the data has been loaded to complete your validation.

[Check answer to Question #487](#)

Question #488

You are an IT Consultant for a top investment bank which is in the process of building its 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. 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.
- B. Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone.
- C. 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.
- D. 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.

[Check answer to Question #488](#)

Question #489

You are working for a commercial bank as an AWS Infrastructure Engineer handling the forex trading application of the bank. You have an Auto Scaling group of EC2 instances that allow your company to cope up with the current demand of traffic and achieve cost-efficiency. You 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 your system from unintended slowdown or unavailability.

Which of the following statements are true regarding the cooldown period? (Select all that applies)

- A. It ensures that before the Auto Scaling group scales out, the EC2 instances have an ample time to cooldown.
- B. It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
- C. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.
- D. Its default value is 300 seconds.
- E. Its default value is 600 seconds.

[Check answer to Question #489](#)

Question #490

You are working as a Solutions Architect for a leading commercial bank which has recently adopted a hybrid cloud architecture. You must ensure that the required data security is in place on all of their AWS resources to meet the strict financial regulatory requirements. In the AWS Shared Responsibility Model, which security aspects are the responsibilities of the customer? (Choose 2)

- A. Managing the underlying network infrastructure
- B. Physical security of hardware
- C. OS Patching of an EC2 instance
- D. IAM Policies and Credentials Management
- E. Virtualization infrastructure

[Check answer to Question #490](#)

Question #491

You are a newly-hired Solutions Architect in a leading utilities provider, which is in the process of migrating their applications to AWS. You created an EBS-Backed EC2 instance with ephemeral0 and ephemeral1 instance store volumes attached to host a web application that fetches and stores data from a web API service.

If this instance is stopped, what will happen to the data on the ephemeral store volumes?

- A. Data is automatically saved in an EBS volume.
- B. Data is unavailable until the instance is restarted.
- C. Data will be deleted.
- D. Data is automatically saved as an EBS snapshot.

[Check answer to Question #491](#)

Question #492

AWS hosts a variety of public datasets such as satellite imagery, geospatial, or genomic data that you want to use for your web application hosted in Amazon EC2. If you use these datasets, how much will it cost you?

- A. A one-time charge of \$10.
- B. \$10 per month for each dataset.
- C. \$10 per month for all datasets.
- D. No charge.

[Check answer to Question #492](#)

Question #493

You are a Solutions Architect of a bank, designing various CloudFormation templates for a new online trading platform that your department will

build.

How much does it cost to use CloudFormation templates?

- A. There is no additional charge for AWS CloudFormation. You only pay for the AWS resources that are created.
- B. The cost is based on the file size of the template.
- C. It is charged per hour.
- D. The cost is based on the size of the template.

[Check answer to Question #493](#)

Question #494

An application 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 and scalability by synchronous data replication to another RDS instance.

Which of the following performs synchronous data replication in RDS?

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

[Check answer to Question #494](#)

Question #495

A company is using Redshift for its online analytical processing (OLAP) application which processes complex queries against large datasets. There is a requirement in which you must define the number of query queues that are available and how queries are routed to those queues for processing.

Which of the following will you use to meet this requirement?

- A. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use RDS database instead.
- B. Create a Lambda function that can accept the number of query queues and use this value to control Redshift.
- C. Use the workload management (WLM) in the parameter group configuration.
- D. This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use a NoSQL DynamoDB database instead.

[Check answer to Question #495](#)

Question #496

You have launched a travel photo sharing website 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 an effective method to mitigate this issue?

- A. Configure your S3 bucket to remove public read access and use pre-signed URLs with expiry dates.
- B. Use CloudFront distributions for your photos.
- C. Block the IP addresses of the offending websites using NACL.
- D. Store photos on an Amazon EBS volume of the web server.

[Check answer to Question #496](#)

Question #497

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? (Choose 2)

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

[Check answer to Question #497](#)

Question #498

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 storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates 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? (Choose 2)

- A. Use 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others.
- B. Setup an AWS Security Token Service to generate temporary tokens.
- C. Use a resource tag on each folder in the S3 bucket.
- D. Configure an IAM role.
- E. Setup up a matching IAM user for each 1200 users in your corporate directory that needs access to a folder in the S3 bucket.

[Check answer to Question #498](#)

Question #499

You have a web-based order processing system which is currently using a queue in Amazon SQS. The support team noticed that there are a lot of cases where an order was processed twice. This issue has caused a lot of trouble in your processing and made your customers very unhappy. Your IT Manager has asked you to ensure that this issue does not happen again. What can you do to prevent this from happening again in the future?

- A. Alter the retention period in Amazon SQS.
- B. Alter the visibility timeout of SQS.
- C. Replace Amazon SQS and instead, use Amazon Simple Workflow service.
- D. Change the message size in SQS.

[Check answer to Question #499](#)

Question #500

You have one security group associated with 10 On-Demand EC2 instances. You configured the security group to allow all inbound SSH traffic and then right after that, you created two new EC2 instances in the same security group. When will the changes be applied to the EC2 instances?

- A. Immediately to all 12 instances in the security group.
- B. Immediately to the new instances only.
- C. Immediately to the new instances, but not for the old ones which must be restarted before the changes take effect.
- D. The changes will apply to all 12 instances after an hour when the propagation is complete.

[Check answer to Question #500](#)

Question #501

Your company is launching a new web portal for its clients. It needs to be launched to a new VPC and will be composed of web servers that will host

the UI app and the REST API services, including two database servers. The web portal will be accessed by the clients through the Internet.

In this scenario, which of the VPC configuration wizard options would you use?

- A. VPC with a Single Public Subnet Only
- B. VPC with Public and Private Subnets
- C. VPC with Public and Private Subnets and Hardware VPN Access
- D. VPC with a Private Subnet Only and Hardware VPN Access
- E. Default VPC

[Check answer to Question #501](#)

Question #502

A startup is in a hurry to build an API for their mobile app to compete with their rival company. Based on their technical requirements, you recommended to build a serverless architecture instead of typically hosting the API in an EC2 instance. Which of the following AWS Services can you use to build and run serverless applications? (Choose 2)

- A. AWS API Gateway
- B. AWS Lambda
- C. ECS
- D. Reserved EC2 Instances
- E. SWF

[Check answer to Question #502](#)

Question #503

You have started your new role as a Solutions Architect for a media company. They host large volumes of data for their operations which are about 250 TB in size on their internal servers. They have decided to store this data on S3 because of its durability and redundancy. The company

currently has a 100 Mbps dedicated line connecting their head office to the Internet. What is the fastest way to import all this data to Amazon S3?

- A. Upload it directly to S3
- B. Use AWS Direct connect and transfer the data over to S3.
- C. Upload the files using AWS Data pipeline.
- D. Use AWS Snowball to upload the files.

[Check answer to Question #503](#)

Question #504

As a Network Architect developing a food ordering application, you need to retrieve the instance ID, public keys, and public IP address of the EC2 server you made for tagging and grouping the attributes into your internal application running on-premises. Which EC2 feature will help you achieve your requirements?

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

[Check answer to Question #504](#)

Question #505

A start-up company that offers an automated transcription service has consulted you about their AWS architecture. They have a fleet of Amazon EC2 worker instances that process an uploaded audio file and then generate a text file as an output.

You must store both uploaded audio and generated text file in the same durable storage until the user has downloaded them. The number of files to be stored can grow over time as the start-up company is expanding rapidly overseas.

Which of the following storage option should you use for this scenario, which is both cost-efficient and scalable?

- A. Amazon Redshift
- B. Amazon Glacier
- C. Amazon S3
- D. Multiple instance stores

[Check answer to Question #505](#)

Question #506

You are building a transcription service for a company in which a fleet of EC2 worker instances process an uploaded audio file and generate a text file as an output. You must store both files in the same durable storage until the text file is retrieved by the uploader. Due to an expected surge in demand, you must ensure that the storage is scalable.

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

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

[Check answer to Question #506](#)

Question #507

A WordPress website hosted in an EC2 instance, which has an additional EBS volume attached, was mistakenly deployed in the us-east-1a Availability Zone due to a misconfiguration in your CloudFormation template. There is a requirement to quickly rectify the issue by moving and attaching the EBS volume to a new EC2 instance in the us-east-1b Availability Zone.

As the Solutions Architect of the company, which of the following should you do to solve this issue?

- A. Create a new EBS volume in another Availability Zone and then specify the current EBS volume as the source.
- B. Detach the EBS volume and attach it to an EC2 instance residing in another Availability Zone.
- C. First, create a snapshot of the EBS volume. Afterwards, create a volume using the snapshot in the other Availability Zone.
- D. First, create a new volume in the other Availability Zone. Next, perform a disk copy of the contents from the source volume to the new volume that you have created.

[Check answer to Question #507](#)

Question #508

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? (Choose 2)

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

[Check answer to Question #508](#)

Question #509

You are working as a Solutions Architect in a startup company which has a project that requires a notification service. You are planning to use Amazon

SNS as it uses a publish/subscribe model for push delivery of messages.

What are the different delivery formats or transports available for receiving notifications from this service? (Choose 2)

- A. Email
- B. CloudFront distribution
- C. File Transfer Protocol
- D. Short Message Service
- E. Simple Network Management Protocol

[Check answer to Question #509](#)

Question #510

You recently created a brand new IAM User with a default setting using AWS CLI. This is intended to be used to send API requests to your S3, DynamoDB, Lambda, and other AWS resources of your cloud infrastructure. Which of the following must be done to allow the user to make API calls to your 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. Assign an IAM Policy to the user to allow it to send API calls.
- D. Create a set of Access Keys for the user.

[Check answer to Question #510](#)

Question #511

Your fellow AWS Engineer has created a new Standard-class S3 bucket to store financial reports that are not frequently accessed but should be immediately available when an auditor request for it. To save costs, you 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? (Choose 2)

- A. It is designed for data that is accessed less frequently.
- B. It is the best storage option to store noncritical and reproducible data.
- C. It is designed for data that requires rapid access when needed.
- D. It provides high latency and low throughput performance.
- E. Ideal to use for data archiving.

[Check answer to Question #511](#)

Question #512

You were hired as an IT Consultant in a startup cryptocurrency company that wants to go global with their international money transfer app. Your project is to make sure that the database of the app is highly available on multiple regions.

What are the benefits of adding Multi-AZ deployments in Amazon RDS? (Choose 2)

- A. It makes the database fault-tolerant to an Availability Zone failure.
- B. Significantly increases the database performance.
- C. Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region.
- D. Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.
- E. Provides SQL optimization.

[Check answer to Question #512](#)

Question #513

You are tasked to host a web application in a new VPC with private and public subnets. In order to do this, you will need to deploy a new MySQL

database server and a fleet of EC2 instances to host the application. In which subnet should you launch the new database server into?

- A. The public subnet
- B. The private subnet
- C. Either public or private subnet
- D. Ideally be launched outside the Amazon VPC

[Check answer to Question #513](#)

Question #514

You are a Solutions Architect in your company working with 3 DevOps Engineers under you. One of the engineers accidentally deleted a file hosted in Amazon S3 which has caused disruption of service. What can you do to prevent this from happening again?

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

[Check answer to Question #514](#)

Question #515

You are working as a Solutions Architect for a start-up company that has a not-for-profit crowdfunding platform hosted in AWS. Their platform allows people around the globe to raise money for social enterprise projects including challenging circumstances like accidents and illnesses.

Since the system handles financial transactions, you must ensure that your cloud architecture is secure. Which of the following AWS services encrypts data at rest by default? (Choose 2)

- A. AWS Storage Gateway

- B. Amazon RDS
- C. Amazon DynamoDB
- D. Amazon Glacier
- E. AWS Lambda

[Check answer to Question #515](#)

Question #516

As a Solutions Architect, you have been requested to set up a highly decoupled application in AWS. Which of the following can help you accomplish this goal?

- A. An SQS queue to allow a second EC2 instance to process a failed instances job
- B. An Elastic Load Balancer to send web traffic to healthy EC2 instances
- C. IAM user credentials on EC2 instances to grant permissions to modify an SQS queue
- D. An Auto Scaling group to recover from EC2 instance failures

[Check answer to Question #516](#)

Question #517

As the Solutions Architect, you have built a photo-sharing site for an entertainment company. The site was hosted using 3 EC2 instances in a single availability zone with a Classic Load Balancer in front to evenly distribute the incoming load. What should you do to enable your Classic Load Balancer to bind a user's session to a specific instance?

- A. Sticky Sessions
- B. Availability Zone
- C. Placement Group
- D. Security Group

[Check answer to Question #517](#)

Question #518

The IT Operations team of your company wants to retrieve all of the Public IP addresses assigned to a running EC2 instance via the Instance metadata. Which of the following URLs will you use?

- A. `http://169.254.169.254/latest/meta-data/public-ipv4`
- B. `http://169.255.169.255/latest/meta-data/public-ipv4`
- C. `http://254.169.254.169/metadata/public-ipv4`
- D. `http://255.169.255.169/latest/public-ipv4`

[Check answer to Question #518](#)

Question #519

You are designing a banking portal which 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 must 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. 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.
- B. Set up a Redis replication group and enable the `AtRestEncryptionEnabled` parameter.
- C. Authenticate the users using Redis AUTH by creating a new Redis Cluster with both the `--transit-encryption-enabled` and `--auth-token` parameters enabled.
- D. Enable the in-transit encryption for Redis replication groups.

[Check answer to Question #519](#)

Question #520

You are building a microservices architecture in which a 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 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.
- C. 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.
- D. 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.

[Check answer to Question #520](#)

Answer to Q1: A

[Go back to Q1](#)

Explanation to Q1

There are three main parts in a distributed messaging system: the components of your distributed system which can be hosted on EC2 instance; your queue (distributed on Amazon SQS servers); and the messages in the queue. To improve the scalability of your distributed system, you can add Auto Scaling group to your EC2 instances.

References :

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html>

[Go back to Q1](#)

Answer to Q2: D, E

[Go back to Q2](#)

Explanation to Q2

In this scenario, enabling IAM cross-account access for all corporate IT administrators in each child account and using AWS Consolidated Billing by creating AWS Organizations to link the divisions accounts to a parent corporate account are the correct choices. The combined use of IAM and Consolidated Billing will support the autonomy of each corporate division while enabling corporate IT to maintain governance and cost oversight.

You can use an IAM role to delegate access to resources that are in different AWS accounts that you own. You share resources in one account with users in a different account. By setting up cross-account access in this way, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources that are in different AWS accounts.

You can use the consolidated billing feature in AWS Organizations to consolidate payment for multiple AWS accounts or multiple AISPL accounts. With consolidated billing, you can see a combined view of AWS charges incurred by all your accounts. You can also get a cost report for each member account that is associated with your master account. Consolidated billing is offered at no additional charge. AWS and AISPL accounts can't be consolidated.

Using AWS Trusted Advisor is incorrect. Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It only provides you alerts on areas where you do not adhere to best practices and tells you how to improve them. It does not assist in maintaining governance over your AWS accounts.

Creating separate VPCs for each division within the corporate IT AWS account is incorrect because creating separate VPCs would not separate the divisions from each other since they will still be operating under the same account and therefore contribute to the same billing each month. Creating separate Availability Zones for each division within the corporate IT AWS account is incorrect because you do not need to create Availability Zones. They are already provided for you by AWS right from the start, and not all services support multiple AZ deployments. In addition, having separate Availability Zones in your VPC does not meet the requirement of supporting the autonomy of each corporate division.

References:

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

[Go back to Q2](#)

Answer to Q3: C

[Go back to Q3](#)

Explanation to Q3

To enable the cross-region replication feature in S3, the following items should be met: The source and destination buckets must have versioning enabled. The source and destination buckets must be in different AWS Regions. Amazon S3 must have permissions to replicate objects from that source bucket to the destination bucket on your behalf. The options that say: The Cross-Region Replication feature is only available for Amazon S3 - RRS and The Cross-Region Replication feature is only available for Amazon S3 - Infrequent Access are incorrect as this feature is available to all types of S3 classes.

The option that says: This is a premium feature which is only for AWS Enterprise accounts is incorrect as this CRR feature is available to all Support Plans.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

[Go back to Q3](#)

Answer to Q4: A

[Go back to Q4](#)

Explanation to Q4

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault-tolerant. They are: Application Load Balancer, Network Load Balancer, and Classic Load Balancer. Network Load Balancer is best suited for load balancing of TCP traffic where extreme performance is required. Operating at the connection level (Layer 4), Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.

Hence, the correct answer is to launch a new Network Load Balancer.

The option that says: Launch a new Application Load Balancer is incorrect because it cannot handle TCP or Layer 4 connections, only Layer 7 (HTTP and HTTPS).

The option that says: Create a new record in Amazon Route 53 with Weighted Routing policy to load balance the incoming traffic is incorrect because although Route 53 can act as a load balancer by assigning each record a relative weight that corresponds to how much traffic you want to send to each resource, it is still not capable of handling millions of requests per second while maintaining ultra-low latencies. You must use a Network Load Balancer instead.

The option that says: Launch a new microservice in AWS Fargate that acts as a load balancer since using an ALB or NLB with Fargate is not possible is incorrect because you can place an ALB and NLB in front of your AWS Fargate cluster.

References:

<https://aws.amazon.com/elasticloadbalancing/features/#compare>

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/load-balancer-types.html>

<https://aws.amazon.com/getting-started/projects/build-modern-app-fargate-lambda-dynamodb-python/module-two/>

[Go back to Q4](#)

Answer to Q5: B

[Go back to Q5](#)

Explanation to Q5

There is no cost if the instance is running and it has only one associated EIP.

[Go back to Q5](#)

Answer to Q6: C

[Go back to Q6](#)

Explanation to Q6

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules. AWS KMS is integrated with most other AWS services that encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs.

By using AWS KMS, you gain more control over access to data you encrypt. You can use the key management and cryptographic features directly in your applications or through AWS services that are integrated with AWS

KMS. Whether you are writing applications for AWS or using AWS services, AWS KMS enables you to maintain control over who can use your customer master keys and gain access to your encrypted data. AWS KMS is integrated with AWS CloudTrail, a service that delivers log files to an Amazon S3 bucket that you designate. By using CloudTrail you can monitor and investigate how and when your master keys have been used and by whom.

If you want a managed service for creating and controlling your encryption keys, but you don't want or need to operate your own HSM, consider using AWS Key Management Service.

Hence, the correct answer is: You should consider using AWS CloudHSM over AWS KMS if you require your keys stored in dedicated, third-party validated hardware security modules under your exclusive control.

The option that says: No major difference. They both do the same thing is incorrect because KMS and CloudHSM are two different services. If you want a managed service for creating and controlling your encryption keys, without operating your own HSM, you must consider using AWS Key Management Service.

The option that says: If you want a managed service for creating and controlling your encryption keys, but you don't want or need to operate your own HSM, consider using AWS CloudHSM is incorrect because you have to consider using AWS KMS if you want a managed service for creating and controlling your encryption keys, without operating your own HSM.

The option that says: AWS CloudHSM should always be used for any payment transactions is incorrect because this is not always the case. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

References:

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>

<https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html>

[Go back to Q6](#)

Answer to Q7: B

[Go back to Q7](#)

Explanation to Q7

AWS offers two kinds of NAT devices a NAT gateway or a NAT instance. It is recommended to use NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI.

Just like a NAT instance, you can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

Here is a diagram showing the differences between NAT gateway and NAT instance:Egress-Only Internet Gateway is incorrect because this is primarily used for VPCs that use IPv6 to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances, just like what NAT Instance and NAT Gateway do. The scenario explicitly says that the EC2 instances are using IPv4 addresses which is why Egress-only Internet gateway is invalid, even though it can provide the required high availability.

VPC Endpoint is incorrect because this simply enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

NAT Instance is incorrect because although this can also enable instances in a private subnet to connect to the Internet or other AWS services and prevent the Internet from initiating a connection with those instances, it is not as highly available compared to a NAT Gateway.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

[Go back to Q7](#)

Answer to Q8: A

[Go back to Q8](#)

Explanation to Q8

It is recommended that you launch the number of instances that you need in the placement group in a single launch request and that you use the same instance type for all instances in the placement group. If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.

If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has capacity for all the requested instances.

The option that says: Stop and restart the instances in the Placement Group and then try the launch again is correct because you can resolve this issue just by launching again. If the instances are stopped and restarted, AWS may move the instances to a hardware that has capacity for all the requested instances.

The option that says: Create another Placement Group and launch the new instances in the new group is incorrect because to benefit from the enhanced networking, all the instances should be in the same Placement Group. Launching the new ones in a new Placement Group will not work in this case.

The option that says: Verify all running instances are of the same size and type and then try the launch again is incorrect because the capacity error is not related to the instance size.

The option that says: Submit a capacity increase request to AWS as you are initially limited to only 12 instances per Placement Group is incorrect because there is no such limit on the number of instances in a Placement Group.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-cluster>

http://docs.amazonaws.cn/en_us/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity

[Go back to Q8](#)

Answer to Q9: B

[Go back to Q9](#)

Explanation to Q9

By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance. The key to managing sticky sessions is to determine how long your load balancer should consistently route the user's request to the same instance. If your application has its own session cookie, then you can configure Elastic Load Balancing so that the session cookie follows the duration specified. If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration.

Reference :

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>

[Go back to Q9](#)

Answer to Q10: D

[Go back to Q10](#)

Explanation to Q10

Apparently, the route table does not have an entry for the Internet Gateway. Therefore, you cannot connect to the EC2 instance. To fix this, you have to add a route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic, and then a target of the Internet gateway ID (igw-xxxxxxxx). This should be the correct route table configuration after adding the new entry.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

[Go back to Q10](#)

Answer to Q11: B

[Go back to Q11](#)

Explanation to Q11

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3. Operating high-performance file systems typically require specialized expertise and administrative overhead, requiring you to provision storage servers and tune complex performance parameters. With Amazon FSx, you can launch and run a file system that provides sub-millisecond access to your data and allows you to read and write data at speeds of up to hundreds of gigabytes per second of throughput and millions of IOPS.

Amazon FSx for Lustre works natively with Amazon S3, making it easy for you to process cloud data sets with high-performance file systems. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write results back to S3. You can also use FSx for Lustre as a standalone high-performance file system to burst your workloads from on-premises to the cloud. By copying on-premises data to an FSx for Lustre file system, you can make that data available for fast processing by compute instances running on AWS. With Amazon FSx, you pay for only the resources you use. There are no minimum commitments, upfront hardware or software costs, or additional fees.

For Windows-based applications, Amazon FSx provides fully managed Windows file servers with features and performance optimized for "lift-and-shift" business-critical application workloads including home directories (user shares), media workflows, and ERP applications. It is accessible from Windows and Linux instances via the SMB protocol. If you have Linux-based applications, Amazon EFS is a cloud-native fully managed file system that provides simple, scalable, elastic file storage accessible from Linux instances via the NFS protocol.

For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that's optimized for performance, with input and output stored on Amazon S3. Hence, the correct answer is: Amazon FSx for Lustre.

Amazon Elastic File System (EFS) is incorrect because although the EFS service can be used for HPC applications, it doesn't natively work with Amazon S3. It doesn't have the capability to easily process your S3 data with a high-performance POSIX interface, unlike Amazon FSx for Lustre.

Amazon FSx for Windows File Server is incorrect because although this service is a type of Amazon FSx, it does not work natively with Amazon S3. This service is a fully managed native Microsoft Windows file system that is primarily used for your Windows-based applications that require shared file storage to AWS.

Amazon Elastic Block Storage (EBS) is incorrect because this service is not a scalable, high-performance file system.

References:

<https://aws.amazon.com/fsx/lustre/>
<https://aws.amazon.com/getting-started/use-cases/hpc/3/>

[Go back to Q11](#)

Answer to Q12: A, C

[Go back to Q12](#)

Explanation to Q12

You can create a snapshot of the instance to save its data and then sell the instance to the Reserved Instance Marketplace. The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in terms of length and pricing options. For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

[Go back to Q12](#)

Answer to Q13: A

[Go back to Q13](#)

Explanation to Q13

In this question, you should take note of this phrase: "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time.

Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

References:

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>
<https://aws.amazon.com/efs/faq/>

[Go back to Q13](#)

Answer to Q14: A

[Go back to Q14](#)

Explanation to Q14

Multicast is a network capability that allows one-to-many distribution of data. With multicasting, one or more sources can transmit network packets to subscribers that typically reside within a multicast group. However, take

note that Amazon VPC does not support multicast or broadcast networking.

You can use an overlay multicast in order to migrate the legacy application. An overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC). Creating a virtual overlay network running on the OS level of the instance is correct because overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC). Provisioning Elastic Network Interfaces between the subnets is incorrect because just providing ENIs between the subnets would not resolve the dependency on multicast.

Creating all the subnets on another VPC and enabling VPC peering is incorrect because VPC peering and multicast are not the same.

The option that says: All the options are correct is incorrect because the only option that will work in this scenario is creating a virtual overlay network.

Reference:

<https://aws.amazon.com/articles/overlay-multicast-in-amazon-virtual-private-cloud>

[Go back to Q14](#)

Answer to Q15: A

[Go back to Q15](#)

Explanation to Q15

For decoupled applications, it is best to use SWF and SQS which are both available in all options. Note that this question asks you for the option that you would LEAST likely to recommend.

SQS polling from an EC2 instance using IAM user credentials is not the recommended way to do so. It should use an IAM role instead.

The rest of the options are the recommended steps to satisfy the given requirement. You must establish first a Direct Connect connection from your data center to your VPC to allow the on-premises servers to connect to SQS. You can either use SWF or SQS to create a decoupled application and you must use an IAM Role, not an IAM user credential, on the EC2 instance to allow polling to the SQS queue.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

[Go back to Q15](#)

Answer to Q16: D

[Go back to Q16](#)

Explanation to Q16

You can choose the credentials that are right for your IAM user. When you use the AWS Management Console to create a user, you must choose to at least include a console password or access keys. By default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. You must create the type of credentials for an IAM user based on the needs of your user.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the

AWS CLI or AWS API (directly or using the AWS SDK). Users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services.

To fill this need, you can create, modify, view, or rotate access keys (access key IDs and secret access keys) for IAM users. When you create an access key, IAM returns the access key ID and secret access key. You should save these in a secure location and give them to the user.

The option that says: Do nothing as the IAM User is already capable of sending API calls to your AWS resources is incorrect because by default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. Take note that in the scenario, you created the new IAM user using the AWS CLI and not via the AWS Management Console, where you must choose to at least include a console password or access keys when creating a new IAM user.

Enabling Multi-Factor Authentication for the user is incorrect because this will still not provide the required Access Keys needed to send API calls to your AWS resources. You must grant the IAM user with Access Keys to meet the requirement.

Assigning an IAM Policy to the user to allow it to send API calls is incorrect because adding a new IAM policy to the new user will not grant the needed Access Keys needed to make API calls to the AWS resources.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html#id_users_creds

[Go back to Q16](#)

Answer to Q17: C

[Go back to Q17](#)

[**Explanation to Q17**](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a group at launch time, the instance is automatically assigned to the default security group for the VPC.

The correct answer is Immediately. Changes made in a security group are immediately implemented. There is no need to wait for some amount of time for propagation nor reboot any instances for your changes to take effect.

The options that say: Roughly around 5-8 minutes in order for the security rules to propagate and It takes exactly one minute for the rules to apply to all availability zones within the AWS region are incorrect because the changes in your security group are implemented immediately and not after a minute or after a few minutes.

The option that says: Immediately after a reboot of the EC2 instances which belong to that security group is incorrect because there is no need to reboot your EC2 instance before the security group changes are fully applied. The change takes effect immediately.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security_Groups.html

[Go back to Q17](#)

Answer to Q18: D

[Go back to Q18](#)

Explanation to Q18

CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, or serverless Lambda functions. It allows you to rapidly release new features, update Lambda function versions, avoid downtime during application deployment, and handle the complexity of updating your applications, without many of the risks associated with error-prone manual deployments.

Creating CloudFormation templates that have the latest configurations and code in them is incorrect since it is used for provisioning and managing stacks of AWS resources based on templates you create to model your infrastructure architecture. CloudFormation is recommended if you want a tool for granular control over the provisioning and management of your own infrastructure.

Using CodeCommit to publish your code quickly in a private repository and pushing them to your resources for fast updates is incorrect as you mainly use CodeCommit for managing a source-control service that hosts private Git repositories. You can store anything from code to binaries and work seamlessly with your existing Git-based tools. CodeCommit integrates with CodePipeline and CodeDeploy to streamline your development and release process.

You could also use OpsWorks to deploy your code, however, creating OpsWorks recipes that will automatically launch resources containing the latest version of the code is still incorrect because you don't need to launch new resources containing your new code when you can just update the ones that are already running.

References:

<https://docs.aws.amazon.com/codedeploy/latest/userguide/deployment-groups.html>

<https://docs.aws.amazon.com/codedeploy/latest/userguide/welcome.html>

Overview of Deployment Options on AWS whitepaper

<https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf>

[Go back to Q18](#)

Answer to Q19: A

[Go back to Q19](#)

[Explanation to Q19](#)

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

Hence, the correct answer is to use Scheduled Reserved Instances, which provide compute capacity that is always available on the specified recurring schedule.

Using On-Demand EC2 instances which allows you to pay for the instances that you launch and use by the second is incorrect because although an On-Demand instance is stable and suitable for processing critical data, it

costs more than any other option. Moreover, the critical financial calculations are only done every night from 10 PM to 3 AM only and not 24/7. This means that your compute capacity will not be utilized for a total of 19 hours every single day.

Using Spot EC2 Instances launched by a persistent Spot request, which can significantly lower your Amazon EC2 costs is incorrect because although this is the most cost-effective solution, this type is not suitable for processing critical financial data since a Spot Instance has a risk of being interrupted.

Using Dedicated Hosts which provide a physical host that is fully dedicated to running your instances, and bringing your existing per-socket, per-core, or per-VM software licenses to reduce costs is incorrect because the use of a fully dedicated physical host is not warranted in this scenario. Moreover, this will be underutilized since you only run the process for 5 hours (from 10 PM to 3 AM only), wasting 19 hours of compute capacity every single day.

References:

<https://aws.amazon.com/blogs/aws/new-scheduled-reserved-instances/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

[Go back to Q19](#)

Answer to Q20: B

[Go back to Q20](#)

[Explanation to Q20](#)

The correct answer is the option that says: Application files are stored in S3. The server log files can also optionally be stored in S3 or in CloudWatch Logs. AWS Elastic Beanstalk stores your application files and optionally, server log files in Amazon S3. If you are using the AWS Management Console, the AWS Toolkit for Visual Studio, or AWS Toolkit for Eclipse, an Amazon S3 bucket will be created in your account and the files you upload will be automatically copied from your local client to Amazon S3.

Optionally, you may configure Elastic Beanstalk to copy your server log files every hour to Amazon S3. You do this by editing the environment configuration settings.

With CloudWatch Logs, you can monitor and archive your Elastic Beanstalk application, system, and custom log files from Amazon EC2 instances of your environments. You can also configure alarms that make it easier for you to react to specific log stream events that your metric filters extract. The CloudWatch Logs agent installed on each Amazon EC2 instance in your environment publishes metric data points to the CloudWatch service for each log group you configure. Each log group applies its own filter patterns to determine what log stream events to send to CloudWatch as data points. Log streams that belong to the same log group share the same retention, monitoring, and access control settings. You can configure Elastic Beanstalk to automatically stream logs to the CloudWatch service.

The option that says: 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 is incorrect because the server log files can also be stored in either S3 or CloudWatch Logs, and not only on the EBS volumes of the EC2 instances which are launched by AWS Elastic Beanstalk.

The option that says: Application files are stored in S3. The server log files can be stored directly in Glacier or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to Glacier. You can create a lifecycle policy to the S3 bucket to store the server logs and archive it in Glacier, but there is no

direct way of storing the server logs to Glacier using Elastic Beanstalk unless you do it programmatically.

The option that says: Application files are stored in S3. The server log files can be optionally stored in CloudTrail or in CloudWatch Logs is incorrect because the server log files can optionally be stored in either S3 or CloudWatch Logs, but not directly to CloudTrail as this service is primarily used for auditing API calls.

Reference:

<https://aws.amazon.com/elasticbeanstalk/faqs/>

[Go back to Q20](#)

Answer to Q21: C

[Go back to Q21](#)

Explanation to Q21

For sub-millisecond latency caching, ElastiCache is the best choice. In order to address scalability and to provide a shared data storage for sessions that can be accessed from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.

ELB sticky sessions is incorrect because the scenario does not require you to route a user to the specific web server that is managing that individual user's session. Since the session state is shared among the instances, the use of the ELB sticky sessions feature is not recommended in this scenario.

Multi-master DynamoDB and Multi-AZ RDS are incorrect because although you can use DynamoDB and RDS for storing session state, these two are not the best choices in terms of cost-effectiveness and performance when compared to ElastiCache. There is a significant difference in terms of latency if you used DynamoDB and RDS when you store the session data.

References:

<https://aws.amazon.com/caching/session-management/>

<https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf>

[Go back to Q21](#)

Answer to Q22: A, E

[Go back to Q22](#)

Explanation to Q22

NA

[Go back to Q22](#)

Answer to Q23: B

[Go back to Q23](#)

Explanation to Q23

Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run.

By using Docker with Elastic Beanstalk, you have an infrastructure that automatically handles the details of capacity provisioning, load balancing,

scaling, and application health monitoring. You can manage your web application in an environment that supports the range of services that are integrated with Elastic Beanstalk, including but not limited to VPC, RDS, and IAM. Hence, AWS Elastic Beanstalk is the correct answer.

ECS is incorrect because although it also provides Service Auto Scaling, Service Load Balancing and Monitoring with CloudWatch, these features are not automatically enabled by default unlike with Elastic Beanstalk. Take note that the scenario requires a service that will automatically handle all the tasks such as balancing load, auto-scaling, monitoring, and placing your containers across your cluster. You will have to manually configure these things if you wish to use ECS. With Elastic Beanstalk, you can manage your web application in an environment that supports the range of services easier.

OpsWorks and AWS CodeDeploy are incorrect because these are primarily used for application deployment and configuration only, without providing load balancing, auto-scaling, monitoring or ECS cluster management.

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html

[Go back to Q23](#)

Answer to Q24: A

[Go back to Q24](#)

Explanation to Q24

If you triggered an S3 API call and got HTTP 200 result code and MD5 checksum, then it is considered as a successful upload. The S3 API will return an error code in case the upload is unsuccessful.

The option that says: Amazon S3 has 99.99999999% durability hence, there is no need to confirm that data was inserted is incorrect because although S3 is durable, it is not an assurance that all objects uploaded using S3 API calls will be successful.

The options that say: You will receive an SMS from Amazon SNS informing you that the object is successfully stored and You will receive an email from Amazon SNS informing you that the object is successfully stored are both incorrect because you don't receive an SMS nor an email notification by default, unless you added an event notification.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html>

[Go back to Q24](#)

Answer to Q25: A

[Go back to Q25](#)

Explanation to Q25

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. It offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of having to wait until all your data are collected before the processing can begin.

Reference:

<https://aws.amazon.com/kinesis/>

[Go back to Q25](#)

Answer to Q26: B

[Go back to Q26](#)

Explanation to Q26

A Lambda function consists of code and any associated dependencies. In addition, a Lambda function also has configuration information associated with it. Initially, you specify the configuration information when you create a Lambda function. Lambda provides an API for you to update some of the configuration data.

You pay for the AWS resources that are used to run your Lambda function. To prevent your Lambda function from running indefinitely, you specify a timeout. When the specified timeout is reached, AWS Lambda terminates execution of your Lambda function. It is recommended that you set this value based on your expected execution time. The default timeout is 3 seconds and the maximum execution duration per request in AWS Lambda is 900 seconds, which is equivalent to 15 minutes.

Hence, the correct answer is the option that says: The failed Lambda functions have been running for over 15 minutes and reached the maximum execution time.

Take note that you can invoke a Lambda function synchronously either by calling the Invoke operation or by using an AWS SDK in your preferred runtime. If you anticipate a long-running Lambda function, your client may time out before function execution completes. To avoid this, update the client timeout or your SDK configuration.

The option that says: The concurrent execution limit has been reached is incorrect because, by default, the AWS Lambda limits the total concurrent executions across all functions within a given region to 1000. By setting a

concurrency limit on a function, Lambda guarantees that allocation will be applied specifically to that function, regardless of the amount of traffic processing the remaining functions. If that limit is exceeded, the function will be throttled but not terminated, which is in contrast with what is happening in the scenario.

The option that says: The Lambda function contains a recursive code and has been running for over 15 minutes is incorrect because having a recursive code in your Lambda function does not directly result to an abrupt termination of the function execution. This is a scenario wherein the function automatically calls itself until some arbitrary criteria is met. This could lead to an unintended volume of function invocations and escalated costs, but not an abrupt termination because Lambda will throttle all invocations to the function.

The option that says: The failed Lambda Invocations contain a ServiceException error which means that the AWS Lambda service encountered an internal error is incorrect because although this is a valid root cause, it is unlikely to have several ServiceException errors throughout the day unless there is an outage or disruption in AWS. Since the scenario says that the Lambda function runs for about 10 to 15 minutes, the maximum execution duration is the most likely cause of the issue and not the AWS Lambda service encountering an internal error.

Reference:

<https://docs.aws.amazon.com/lambda/latest/dg/limits.html>

<https://docs.aws.amazon.com/lambda/latest/dg/resource-model.html>

[Go back to Q26](#)

Answer to Q27: B

[Go back to Q27](#)

Explanation to Q27

By default, records of a stream in Amazon Kinesis are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention.

The option that says: Amazon S3 bucket has encountered a data loss is incorrect because Amazon S3 rarely experiences data loss. Amazon has an SLA for S3 that it commits to its customers. Amazon S3 Standard, S3 StandardIA, S3 One Zone-IA, and S3 Glacier are all designed to provide 99.99999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects. Hence, Amazon S3 bucket data loss is highly unlikely.

The option that says: Someone has manually deleted the record in Amazon S3 is incorrect because if someone has deleted the data, this should have been visible in CloudTrail. Also, deleting that much data manually shouldn't have occurred in the first place if you have put in the appropriate security measures.

The option that says: The access of the Kinesis stream to the S3 bucket is insufficient is incorrect because having insufficient access is highly unlikely since you are able to access the bucket and view the contents of the previous day's data collected by Kinesis.

Reference:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html>

[Go back to Q27](#)

Answer to Q28: A

[Go back to Q28](#)

Explanation to Q28

Using AWS Organizations and Service Control Policies to control services on each account is the correct answer.

AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It allows you to create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts.

Setting up a common IAM policy that can be applied across all AWS accounts is incorrect because it is not possible to create a common IAM policy for multiple AWS accounts.

The option that says: 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 is incorrect because although you can set up cross-account access to each department, this entails a lot of configuration compared with using AWS Organizations and Service Control Policies (SCPs). Cross-account access would be a more suitable choice if you only have two accounts to manage, but not for multiple accounts.

The option that says: 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 is incorrect as this option is focused on the Identity Federation authentication set up for your AWS accounts but not the IAM policy management for multiple AWS accounts. A combination of AWS Organizations and Service Control Policies (SCPs) is a better choice compared to this option.

Reference:

<https://aws.amazon.com/organizations/>

[Go back to Q28](#)

Answer to Q29: C

[Go back to Q29](#)

Explanation to Q29

NA

[Go back to Q29](#)

Answer to Q30: D

[Go back to Q30](#)

Explanation to Q30

To control the versions of files that are served from your distribution, you can either invalidate files or give them versioned file names. If you want to update your files frequently, AWS recommends that you primarily use file versioning for the following reasons:

- Versioning enables you to control which file a request returns even when the user has a version cached either locally or behind a corporate caching proxy. If you invalidate the file, the user might continue to see the old version until it expires from those caches.
- CloudFront access logs include the names of your files, so versioning makes it easier to analyze the results of file changes.
- Versioning provides a way to serve different versions of files to different users.- Versioning simplifies rolling forward and back between file

revisions.

- Versioning is less expensive. You still must pay for CloudFront to transfer new versions of your files to edge locations, but you don't have to pay for invalidating files.

Invalidating the files in your CloudFront web distribution is incorrect because even though using invalidation will solve this issue, this solution is more expensive as compared to using versioned objects.

Adding a separate cache behavior path for the content and configuring a custom object caching with a Minimum TTL of 0 is incorrect because this alone is not enough to solve the problem. A cache behavior is primarily used to configure a variety of CloudFront functionality for a given URL path pattern for files on your website. Although this solution may work, it is still better to use versioned objects where you can control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

Adding Cache-Control no-cache, no-store, or private directives in the S3 bucket is incorrect because although it is right to configure your origin to add the Cache-Control or Expires header field, you should do this to your objects and not on the entire S3 bucket.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/UpdatingExistingObjects.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/prevent-cloudfront-from-caching-files/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html#PayingForInvalidation>

[Go back to Q30](#)

Answer to Q31: A

[Go back to Q31](#)

Explanation to Q31

The best option is to create a role in IAM. Afterwards, assign this role to a new EC2 instance. Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances.

You can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

In this scenario, you must use IAM roles so that your applications can securely make API requests from your instances without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

Encrypting the API credentials and storing in any directory of the EC2 instance and storing the API credentials in the root web application directory of the EC2 instance are incorrect. Though you can store and use the API credentials in the EC2 instance, it will be difficult to manage just as mentioned above. You must use IAM Roles.

Storing your API credentials in Amazon S3 Glacier is incorrect as Amazon S3 Glacier is used for data archives and not for managing API credentials.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

[Go back to Q31](#)

Answer to Q32: D

[Go back to Q32](#)

Explanation to Q32

One thing that you should notice here is that the company is using Multi-AZ databases in all their environments, including their development and test environment.

This is costly and unnecessary as these two environments are not critical. It is better to use Multi-AZ for production environments to reduce costs, which is why the option that says: Consider not using a Multi-AZ RDS deployment for the development and test database is the correct answer.

The option that says: Consider using On-demand instances instead of Reserved EC2 instances is incorrect because selecting Reserved instances is cheaper than On-demand instances for long term usage due to the discounts offered when purchasing reserved instances.

The option that says: Consider using Spot instances instead of reserved EC2 instances is incorrect because the web servers are running in a production environment. Never use Spot instances for production level web servers unless you are sure that they are not that critical in your system. This is because your spot instances can be terminated once the maximum price goes over the maximum amount that you specified.

The option that says: Consider removing the Elastic Load Balancer is incorrect because the Elastic Load Balancer is crucial in maintaining the elasticity and reliability of your system.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>
<https://aws.amazon.com/pricing/cost-optimization/>

[Go back to Q32](#)

Answer to Q33: A, E

[Go back to Q33](#)

Explanation to Q33

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.

The option that says: When you need a low packet-per-second performance is incorrect because you want to increase packet-per-second performance, and not lower it, when you enable enhanced networking.

The option that says: When you need high latency, networking is incorrect because higher latencies means slower network, which is the opposite of what you want to happen when you enable enhanced networking.

The option that says: When you need a dedicated connection to your on-premises data center is incorrect because enabling enhanced networking does not provide a dedicated connection to your on-premises data center. Use AWS Direct Connect or enable VPN tunneling instead for this purpose.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

[Go back to Q33](#)

Answer to Q34: A

[Go back to Q34](#)

Explanation to Q34

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a group at launch time, the instance is automatically assigned to the default security group for the VPC.

For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things you need to know about security groups for your VPC and their rules.

You can add or remove rules for a security group which is also referred to as authorizing or revoking inbound or outbound access. A rule applies either to inbound traffic (ingress) or outbound traffic (egress). You can grant access to a specific CIDR range, or to another security group in your VPC or in a peer VPC (requires a VPC peering connection). In the scenario, the servers of the application-tier are in an Auto Scaling group which means that the number of EC2 instances could grow or shrink over time. An Auto Scaling group could also cover one or more Availability Zones (AZ) which have their own subnets. Hence, the most suitable solution would be

to set up the security group of the database tier to allow database traffic from the security group of the application servers since you can utilize the security group of the application-tier Auto Scaling group as the source for the security group rule in your database tier.

Setting up the security group of the database tier to allow database traffic from a specified list of application server IP addresses is incorrect because the list of application server IP addresses will change over time since an Auto Scaling group can add or remove EC2 instances based on the configured scaling policy. This will create inconsistencies in your application because the newly launched instances, which are not included in the initial list of IP addresses, will not be able to access the database.

Setting up the Network ACL of the database subnet to deny all inbound non-database traffic from the subnet of the application-tier is incorrect because doing this could affect the other EC2 instances of other applications, which are also hosted in the same subnet of the application-tier. For example, a large subnet with a CIDR block of /16 could be shared by several applications. Denying all inbound non-database traffic from the entire subnet will impact other applications which use this subnet.

Setting up the Network ACL of the database subnet to allow inbound database traffic from the subnet of the application-tier is incorrect because although this solution can work, the subnet of the application-tier could be shared by another tier or another set of EC2 instances other than the application-tier. This means that you would inadvertently be granting database access to unauthorized servers hosted in the same subnet other than the application-tier.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security_Groups.html

[Go back to Q34](#)

Answer to Q35: A

[Go back to Q35](#)

Explanation to Q35

In EC2-Classic, your EC2 instance receives a private IPv4 address from the EC2-Classic range each time it's started. In EC2-VPC on the other hand, your EC2 instance receives a static private IPv4 address from the address range of your default VPC. Hence, the correct answer is launching the instances in the Amazon Virtual Private Cloud (VPC) and not launching the instances in EC2-Classic. Launching the instances to a single Availability Zone and launching the instances to multiple Availability Zones are incorrect due to the fact that Availability Zones do not provide static private IP addresses to EC2 instances.

Launching the instances in a Placement Group is incorrect as a Placement Group is just a grouping of instances.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-classic-platform.html#differences-ec2-classic-vpc>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>

[Go back to Q35](#)

Answer to Q36: B

[Go back to Q36](#)

Explanation to Q36

NA

[Go back to Q36](#)

Answer to Q37: A, E

[Go back to Q37](#)

Explanation to Q37

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

The chief benefits of running your DB instance as a Multi-AZ deployment are enhanced database durability and availability. The increased availability and fault tolerance offered by Multi-AZ deployments make them a natural fit for production environments.

Hence, the correct answers are the following options:- Increased database availability in the case of system upgrades like OS patching or DB Instance scaling.- Provides enhanced database durability in the event of a DB instance component failure or an Availability Zone outage.

The option that says: Creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ) in a different region is almost correct. RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ) that is in the same region and not in a different one.

The options that say: Significantly increases the database performance and Provides SQL optimization are incorrect as it does not affect the performance nor provide SQL optimization.

References:

<https://aws.amazon.com/rds/details/multi-az/>
<https://aws.amazon.com/rds/faqs/>

[Go back to Q37](#)

Answer to Q38: A

[Go back to Q38](#)

Explanation to Q38

Using MyISAM as the storage engine for MySQL is not recommended. The recommended storage engine for MySQL is InnoDB and not MyISAM.

The rest of the options are best practices in the AWS MySQL RDS documentation. Again, InnoDB is the recommended storage engine for MySQL. However, in case you require intense, full-text search capability, use MyISAM storage engine instead.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html#CHAP_BestPractices.MySQLStorage

[Go back to Q38](#)

Answer to Q39: B

[Go back to Q39](#)

Explanation to Q39

You can use path conditions to define rules that forward requests to different target groups based on the URL in the request (also known as path-based routing). This type of routing is the most appropriate solution for this scenario hence, using path conditions to define rules that forward requests to different target groups based on the URL in the request is the correct answer.

Each path condition has one path pattern. If the URL in a request matches the path pattern in a listener rule exactly, the request is routed using that rule.

A path pattern is case-sensitive, can be up to 128 characters in length, and can contain any of the following characters. You can include up to three wildcards characters.AZ, az, 09_ - . \$ / ~ " ' @ : +& (using &)* (matches 0 or more characters)? (matches exactly 1 character)Example path patterns/img/*/js/*

The option that says: Use host conditions to define rules that forward requests to different target groups based on the host name in the host header. This enables you to support multiple domains using a single load balancer is incorrect because host-based routing defines rules that forward requests to different target groups based on the host name in the host header instead of the URL, which is what is needed in this scenario.

The option that says: Replace your ALB with a Classic Load Balancer then use path conditions to define rules that forward requests to different target groups based on the URL in the request is incorrect because a Classic Load

Balancer does not support path-based routing. You must use an Application Load Balancer.

The option that says: 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 is incorrect because a Network Load Balancer is used for applications that need extreme network performance and static IP. It also does not support path-based routing which is what is needed in this scenario. Furthermore, the statement mentions host-based routing yet, the description is about path-based routing.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-benefits>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#path-conditions>

[Go back to Q39](#)

Answer to Q40: C, E

[Go back to Q40](#)

Explanation to Q40

You can connect your VPC to remote networks by using a VPN connection which can be Direct Connect, IPsec VPN connection, AWS VPN CloudHub, or a third-party software VPN appliance. Hence, IPsec VPN connection and AWS Direct Connect are the correct answers.

Amazon Connect is incorrect because this is not a VPN connectivity option. It is a self-service, cloud-based contact center service in AWS that makes it

easy for any business to deliver better customer service at a lower cost. Amazon Connect is based on the same contact center technology used by Amazon customer service associates around the world to power millions of customer conversations.

VPC Peering is incorrect because this is a networking connection between two VPCs only, which enables you to route traffic between them privately. This can't be used to connect your on-premises network to your VPC.NAT Gateway is incorrect because you only use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances. This is not used to connect to your on-premises network.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

<https://aws.amazon.com/connect/>

[Go back to Q40](#)

Answer to Q41: D

[Go back to Q41](#)

Explanation to Q41

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can write and run scripts that install new packages, software, or tools in your instance when it is launched.

You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives. You can also pass this data into the launch wizard as plain text, as a file (this is useful for launching instances using the command line tools), or as base64-encoded text (for API calls).

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>

[Go back to Q41](#)

Answer to Q42: D

[Go back to Q42](#)

Explanation to Q42

Storage Optimized Instances is the correct answer. Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

Memory Optimized Instances is incorrect because these are designed to deliver fast performance for workloads that process large data sets in memory, which is quite different from handling high read and write capacity on local storage.

Compute Optimized Instances is incorrect because these are ideal for compute-bound applications that benefit from high-performance processors, such as batch processing workloads and media transcoding.

General Purpose Instances is incorrect because these are the most basic type of instances. They provide a balance of compute, memory, and networking resources, and can be used for a variety of workloads. Since

you are requiring higher read and write capacity, storage optimized instances should be selected instead.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html>

[Go back to Q42](#)

Answer to Q43: B

[Go back to Q43](#)

Explanation to Q43

In this scenario, the main culprit is that the Cache-Control max-age directive is set to a low value, which is why the request is always directed to your origin server.

Hence the correct answer is the option that says: The Cache-Control max-age directive is set to zero.

The option that says: 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 is incorrect because the issue also occurs even for the commonly requested objects. This means that these objects were successfully requested before but due to a zero Cache-Control max-age directive value, it causes this issue in CloudFront.

The options that say: The file sizes of the cached objects are too large for CloudFront to handle and You did not add an SSL certificate are incorrect because they are not related to the issue in caching.

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

Typically, CloudFront serves an object from an edge location until the cache duration that you specified passes that is, until the object expires. After it expires, the next time the edge location gets a user request for the object, CloudFront forwards the request to the origin server to verify that the cache contains the latest version of the object.

The Cache-Control and Expires headers control how long objects stay in the cache. The Cache-Control max-age directive lets you specify how long (in seconds) you want an object to remain in the cache before CloudFront gets the object again from the origin server. The minimum expiration time CloudFront supports is 0 seconds for web distributions and 3600 seconds for RTMP distributions.

Reference:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>

[Go back to Q43](#)

Answer to Q44: A

[Go back to Q44](#)

Explanation to Q44

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region

that provides the lowest latency.

You can create latency records for your resources in multiple AWS Regions by using latency-based routing. In the event that Route 53 receives a DNS query for your domain or subdomain such as techrad.io or portal.techrad.io, it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency and then selects a latency record for that region. Route 53 responds with the value from the selected record which can be the IP address for a web server or the CNAME of your elastic load balancer.

Hence, using Route 53 to distribute the load to the multiple EC2 instances across all AWS Regions is the correct answer.

Using a Network Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions and using an Application Load Balancer to distribute the load to the multiple EC2 instances across all AWS Regions are both incorrect because load balancers distribute traffic only within their respective regions and not to other AWS regions by default. Although Network Load Balancers support connections from clients to IP-based targets in peered VPCs across different AWS Regions, the scenario didn't mention that the VPCs are peered with each other. It is best to use Route 53 instead to balance the incoming load to two or more AWS regions more effectively.

Using AWS DataSync to distribute the load to the multiple EC2 instances across all AWS Regions is incorrect because the AWS DataSync service simply provides a fast way to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS).

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialAddingLBRRegion.html>

[Go back to Q44](#)

Answer to Q45: B

[Go back to Q45](#)

[Explanation to Q45](#)

With web identity federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account. Using an IdP helps you keep your AWS account secure because you don't have to embed and distribute long-term security credentials with your application.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

[Go back to Q45](#)

Answer to Q46: A

[Go back to Q46](#)

[Explanation to Q46](#)

Using Redis AUTH command can improve data security by requiring the user to enter a password before they are granted permission to execute Redis commands on a password-protected Redis server.

Hence, the correct answer is to authenticate the users using Redis AUTH by creating a new Redis Cluster with both the --transit-encryption-enabled and --auth-token parameters enabled.

To require that users enter a password on a password-protected Redis server, include the parameter --auth-token with the correct password when you create your replication group or cluster and on all subsequent commands to the replication group or cluster.

Enabling the in-transit encryption for Redis replication groups is incorrect because although in-transit encryption is part of the solution, it is missing the most important thing which is the Redis AUTH option.

Creating a new Redis replication group and setting the AtRestEncryptionEnabled parameter to true is incorrect because the Redis At-Rest Encryption feature only secures the data inside the in-memory data store. You must use Redis AUTH option instead.

The option that says: Do nothing. This feature is already enabled by default is incorrect because the Redis AUTH option is disabled by default.

References:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html>

[Go back to Q46](#)

Answer to Q47: D

[Go back to Q47](#)

Explanation to Q47

An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet and prevents the Internet from initiating an IPv6 connection with your instances.

Take note that an egress-only Internet gateway is for use with IPv6 traffic only. To enable outbound-only Internet communication over IPv4, use a NAT gateway instead.

NAT Gateway and NAT instances are incorrect because these are only applicable for IPv4 and not IPv6. Even though these two components can enable the EC2 instance in a private subnet to communicate to the Internet and prevent inbound traffic, it is only limited with instances which are using IPv4 address and not IPv6. The most suitable VPC component to use is egress-only Internet gateway.

Internet Gateway is incorrect because this is primarily used to provide Internet access to your instances in the public subnet of your VPC, and not for private subnets. However, with an Internet gateway, traffic originating from the public Internet will also be able to reach your instances. The scenario is asking you to prevent inbound access, so this is not the correct answer.

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

[Go back to Q47](#)

Answer to Q48: A

[Go back to Q48](#)

Explanation to Q48

In CloudFormation, a template is a JSON or a YAML-formatted text file that describes your AWS infrastructure. Templates include several major sections. The Resources section is the only required section. Some sections in a template can be in any order. However, as you build your template, it might be helpful to use the logical ordering of the following list, as values in one section might refer to values from a previous section. Take note that all the sections here are optional, except for Resources, which is the only one required.

- Format Version
- Description
- Metadata
- Parameters
- Mappings
- Conditions
- Transform
- Resources (required)
- Outputs

Reference:

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/tempalte-anatomy.html>

[Go back to Q48](#)

Answer to Q49: D

[Go back to Q49](#)

Explanation to Q49

Amazon Aurora MySQL and Amazon Aurora PostgreSQL support Amazon Aurora Replicas, which share the same underlying volume as the primary instance. Updates made by the primary are visible to all Amazon Aurora Replicas. With Amazon Aurora MySQL, you can also create MySQL Read Replicas based on MySQL's binlog-based replication engine. In MySQL Read Replicas, data from your primary instance is replayed on your replica as transactions. For most use cases, including read scaling and high availability, it is recommended using Amazon Aurora Replicas.

Read Replicas are primarily used for improving the read performance of the application. The most suitable solution in this scenario is to use Multi-AZ deployments instead but since this option is not available, you can still

set up Read Replicas which you can promote as your primary stand-alone DB cluster in the event of an outage.

Hence, the correct answer here is to create Amazon Aurora Replicas.

Deploying Aurora to two Auto-Scaling groups of EC2 instances across two Availability Zones with an elastic load balancer which handles load balancing is incorrect because Aurora is a managed database engine for RDS and not deployed on typical EC2 instances that you manually provision.

Enabling Hash Joins to improve the database query performance is incorrect because Hash Joins are mainly used if you need to join a large amount of data by using an equijoin and not for improving availability.

Using an Asynchronous Key Prefetch in Amazon Aurora to improve the performance of queries that join tables across indexes is incorrect because the Asynchronous Key Prefetch is mainly used to improve the performance of queries that join tables across indexes.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQLBestPractices.html>

<https://aws.amazon.com/rds/aurora/faqs/>

[Go back to Q49](#)

Answer to Q50: B

[Go back to Q50](#)

[Explanation to Q50](#)

NA

[Go back to Q50](#)

Answer to Q51: D

[Go back to Q51](#)

Explanation to Q51

You should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use an IAM role, you don't have to distribute long-term credentials (such as a username and password or access keys) to an EC2 instance.

Instead, the role supplies temporary permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.

Hence, the best option here is to remove the stored access keys first in the AMI. Then, create a new IAM role with permissions to access the DynamoDB table and assign it to the EC2 instances.

Putting the access keys in Amazon Glacier or in an Amazon S3 bucket are incorrect because S3 and Glacier are mainly used as a storage option. It is better to use an IAM role instead of storing access keys in these storage services.

The option that says: Do nothing. The architecture is already secure because the access keys are already in the Amazon Machine Image is incorrect because you can make the architecture more secure by using IAM.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html

[Go back to Q51](#)

Answer to Q52: D

[Go back to Q52](#)

Explanation to Q52

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. It is designed to deliver 99.99999999% durability and provides comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements. Amazon Glacier provides query-in-place functionality, allowing you to run powerful analytics directly on your archive data at rest.

Reference:

<https://aws.amazon.com/glacier/faqs/>

[Go back to Q52](#)

Answer to Q53: C

[Go back to Q53](#)

Explanation to Q53

Amazon Route 53 DNS services does not support DNSSEC currently. However, their domain name registration service supports configuration of signed DNSSEC keys for domains when DNS service is configured at another provider. More information on configuring DNSSEC for your domain name registration can be found here. Amazon Route 53 currently supports the following DNS record types:

- A (address record)
- AAAA (IPv6 address record)
- CNAME (canonical name record)
- CAA (certification authority authorization)
- MX (mail exchange record)
- NAPTR (name authority pointer record)
- NS (name server record)
- PTR (pointer record)
- SOA (start of authority record)
- SPF (sender policy framework)
- SRV (service locator)
- TXT (text record)

Reference:

<https://aws.amazon.com/route53/faqs/>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html>

[Go back to Q53](#)

Answer to Q54: B

[Go back to Q54](#)

Explanation to Q54

NA

[Go back to Q54](#)

Answer to Q55: A

[Go back to Q55](#)

Explanation to Q55

The main issue is the slow upload time of the video objects to Amazon S3. To address this issue, you can use Multipart upload in S3 to improve the throughput. It allows you to upload parts of your object in parallel thus, decreasing the time it takes to upload big objects. Each part is a contiguous portion of the object's data.

You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

Using multipart upload provides the following advantages: Improved throughput - You can upload parts in parallel to improve throughput.

Quick recovery from any network issues - Smaller part size minimizes the impact of restarting a failed upload due to a network error.

Pause and resume object uploads - You can upload object parts over time. Once you initiate a multipart upload, there is no expiry; you must explicitly complete or abort the multipart upload.

Begin an upload before you know the final object size - You can upload an object as you are creating it.

Enabling Enhanced Networking with the Elastic Network Adapter (ENA) on your EC2 Instances is incorrect because even though this will improve network performance, the issue will persist since the problem lies in the upload time of the object to Amazon S3. You should use the Multipart upload feature instead.

Leveraging on Amazon CloudFront and using HTTP POST method to reduce latency is incorrect because CloudFront is a CDN service and is not used to expedite the upload process of objects to Amazon S3. Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

Using Amazon Elastic Block Store Provisioned IOPS and an Amazon EBS-optimized instance is incorrect because although the use of Amazon Elastic Block Store Provisioned IOPS will speed up the I/O performance of the EC2 instance, the root cause is still not resolved since the primary problem here is the slow video upload to Amazon S3. There is no network contention in the EC2 instance.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html>

<http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html>

[Go back to Q55](#)

Answer to Q56: C

[Go back to Q56](#)

Explanation to Q56

With AWS Lambda, you pay only for what you use. You are charged based on the number of requests for your functions and the duration, the time it

takes for your code to execute.

Lambda counts a request each time it starts executing in response to an event notification or invoke call, including test invokes from the console. You are charged for the total number of requests across all your functions. Duration is calculated from the time your code begins executing until it returns or otherwise terminates, rounded up to the nearest 100ms. The price depends on the amount of memory you allocate to your function. The Lambda free tier includes 1M free requests per month and over 400,000 GB-seconds of compute time per month.

The best possible answer here is to use Lambda and API Gateway because this solution is both scalable and cost-effective. You will only be charged when you use your Lambda function, unlike having an EC2 instance which always runs even though you don't use it.

Setting up a micro-service architecture with ECS, ECR, and Fargate is incorrect because ECS is mainly used to host Docker applications and in addition, using ECS, ECR, and Fargate alone is not scalable and not recommended for this type of scenarios.

Hosting the APIs in a static S3 web hosting bucket behind a CloudFront web distribution is not a suitable option as there is no compute capability for S3 and you can only use it as a static website. Although this solution is scalable since it is using CloudFront, the use of S3 to host the web APIs or the dynamic website is still incorrect.

The option that says: 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 is incorrect because EC2 alone, without Auto Scaling, is not scalable. Even though you use Spot EC2 instance, it is still more expensive compared to Lambda because you will be charged only when your function is being used. An Elastic Fabric Adapter (EFA) is simply a network device that you can attach to your Amazon EC2 instance that enables you to achieve the application performance of an on-premises HPC

cluster, with the scalability, flexibility, and elasticity provided by the AWS Cloud. Although EFA is scalable, the Spot Fleet configuration of this option doesn't have Auto Scaling involved.

References:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html>

<https://aws.amazon.com/lambda/pricing/>

[Go back to Q56](#)

Answer to Q57: A, E

[Go back to Q57](#)

Explanation to Q57

In this scenario, you can use CloudWatch to monitor your AWS resources and SNS to provide notification. Hence, the correct answers are CloudWatch and Amazon Simple Notification Service.

Amazon Simple Notification Service (SNS) is a flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. SWF is incorrect because this is mainly used for managing workflows and not for monitoring and notifications.

Amazon Simple Queue Service is incorrect because this is a messaging queue service and not suitable for this kind of scenario.

Route 53 is incorrect because this is primarily used for routing and domain name registration and management.

References:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html

<https://aws.amazon.com/sns/>

[Go back to Q57](#)

Answer to Q58: C

[Go back to Q58](#)

Explanation to Q58

NA

[Go back to Q58](#)

Answer to Q59: B

[Go back to Q59](#)

Explanation to Q59

CloudWatch Logs agent provides an automated way to send log data to CloudWatch Logs from Amazon EC2 instances hence, CloudWatch Logs agent is the correct answer.

The CloudWatch Logs agent is comprised of the following components:- A plug-in to the AWS CLI that pushes log data to CloudWatch Logs.- A script (daemon) that initiates the process to push data to CloudWatch Logs.- A cron job that ensures that the daemon is always running.

CloudTrail is incorrect as this is mainly used for tracking the API calls of your AWS resources and not for sending EC2 logs to CloudWatch.

VPC Flow Logs is incorrect as this is mainly used for tracking the traffic coming into the VPC and not for EC2 instance monitoring.

CloudTrail Logs agent is incorrect because this does not exist.

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html>

[Go back to Q59](#)

Answer to Q60: D

[Go back to Q60](#)

Explanation to Q60

Since you are using a Remote Desktop connection to access your EC2 instance, you must ensure that the Remote Desktop Protocol is allowed in the security group. By default, the server listens on TCP port 3389 and UDP port 3389.

The option that says: You should adjust the security group to allow traffic from port 22 is incorrect as the port 22 is used for SSH connections and not for RDP.

The options that say: You should restart the EC2 instance since there might be some issue with the instance and You should create a new instance since there might be some issue with the instance are incorrect as the EC2 instance is newly created and hence, unlikely to cause the issue. You must check the security group first if it allows the Remote Desktop Protocol (3389) before investigating if there is indeed an issue on the specific instance.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/troubleshooting-windows-instances.html#rdp-issues>

[Go back to Q60](#)

Answer to Q61: A

[Go back to Q61](#)

Explanation to Q61

The first step is to create a snapshot of the EBS volume. Create a volume using this snapshot and then specify the new Availability Zone accordingly.

A point-in-time snapshot of an EBS volume, can be used as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental only, the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the entire volume.

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or

subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

Creating a new EBS volume in another Availability Zone and then specifying the current EBS volume as the source is incorrect. There is no such action like this in AWS since EBS volumes do not require a source from other EBS volumes.

Detaching the EBS volume and attaching it to an EC2 instance residing in another Availability Zone is incorrect because an EBS volume is only available in the Availability Zone it was created in and cannot be attached directly to other Availability Zones.

The option that says: First, create a new volume in the other Availability Zone. Next, perform a disk copy of the contents from the source volume to the new volume that you have created is incorrect because doing that is not the safest way to copy EBS contents. Create a snapshot instead for better reliability of the process.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html>

[Go back to Q61](#)

Answer to Q62: A

[Go back to Q62](#)

[Explanation to Q62](#)

In this scenario, the best option is to use IAM Role to provide access. You can create a new IAM Role then associate it to the IAM user. Attach a policy allowing access to modify the ELB and once it is done, remove the IAM role to the user.

An IAM role is like a user in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

[Go back to Q62](#)

Answer to Q63: D

[Go back to Q63](#)

Explanation to Q63

The right answer is to enable cross-zone load balancing.

If the load balancer nodes for your Classic Load Balancer can distribute requests regardless of Availability Zone, this is known as cross-zone load balancing. With cross-zone load balancing enabled, your load balancer nodes distribute incoming requests evenly across the Availability Zones enabled for your load balancer. Otherwise, each load balancer node distributes requests only to instances in its Availability Zone.

For example, if you have 10 instances in Availability Zone us-west-2a and 2 instances in us-west-2b, the requests are distributed evenly across all 12 instances if cross-zone load balancing is enabled. Otherwise, the 2 instances in us-west-2b serve the same number of requests as the 10 instances in us-west-2a. Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances. However, we still recommend that you maintain approximately equivalent numbers of instances in each enabled Availability Zone for higher fault tolerance.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html>

[Go back to Q63](#)

Answer to Q64: A, B

[Go back to Q64](#)

Explanation to Q64

You can use Secure Sockets Layer (SSL) to encrypt connections between your client applications and your Amazon RDS DB instances running Microsoft SQL Server. SSL support is available in all AWS regions for all supported SQL Server editions.

When you create an SQL Server DB instance, Amazon RDS creates an SSL certificate for it. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

There are 2 ways to use SSL to connect to your SQL Server DB instance:-
Force SSL for all connections this happens transparently to the client, and the client doesn't have to do any work to use SSL.- Encrypt specific connections this sets up an SSL connection from a specific client computer, and you must do work on the client to encrypt connections.

You can force all connections to your DB instance to use SSL, or you can encrypt connections from specific client computers only. To use SSL from a specific client, you must obtain certificates for the client computer, import certificates on the client computer, and then encrypt the connections from the client computer.

If you want to force SSL, use the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to false. Set the `rds.force_ssl` parameter to true to force connections to use SSL. The `rds.force_ssl` parameter is static, so after you change the value, you must reboot your DB instance for the change to take effect.

Hence, the correct answers for this scenario are the options that say:-
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.- 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.

Specifying the TDE option in an RDS option group that is associated with that DB instance to enable transparent data encryption (TDE) is incorrect

because transparent data encryption (TDE) is primarily used to encrypt stored data on your DB instances running Microsoft SQL Server, and not the data that are in transit.

Enabling the IAM DB authentication in RDS using the AWS Management Console is incorrect because IAM database authentication is only supported in MySQL and PostgreSQL database engines. With IAM database authentication, you don't need to use a password when you connect to a DB instance but instead, you use an authentication token.

Configuring the security groups of your EC2 instances and RDS to only allow traffic to and from port 443 is incorrect because it is not enough to do this. You need to either force all connections to your DB instance to use SSL, or you can encrypt connections from specific client computers, just as mentioned above.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServerConcepts.General.SSL.Using.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

[Go back to Q64](#)

Answer to Q65: C

[Go back to Q65](#)

[Explanation to Q65](#)

Amazon Kinesis Data Streams supports resharding, which lets you adjust the number of shards in your stream to adapt to changes in the rate of data flow through the stream. Resharding is considered an advanced operation.

There are two types of resharding operations: shard split and shard merge. In a shard split, you divide a single shard into two shards. In a shard merge, you combine two shards into a single shard. Resharding is always pairwise in the sense that you cannot split into more than two shards in a single operation, and you cannot merge more than two shards in a single operation. The shard or pair of shards that the resharding operation acts on are referred to as parent shards. The shard or pair of shards that result from the resharding operation are referred to as child shards.

Splitting increases the number of shards in your stream and therefore increases the data capacity of the stream. Because you are charged on a per-shard basis, splitting increases the cost of your stream. Similarly, merging reduces the number of shards in your stream and therefore decreases the data capacity and cost of the stream.

If your data rate increases, you can also increase the number of shards allocated to your stream to maintain the application performance. You can reshuffle your stream using the `UpdateShardCount` API. The throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream. Hence, the correct answer is to increase the number of shards of the Kinesis stream by using the `UpdateShardCount` command.

Replacing the data stream with Amazon Kinesis Data Firehose instead is incorrect because the throughput of Kinesis Firehose is not exceptionally higher than Kinesis Data Streams. In fact, the throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream.

Improving the performance of the stream by decreasing the number of its shards using the `MergeShard` command is incorrect because merging the

shards will effectively decrease the performance of the stream rather than improve it.

Implementing Step Scaling to the Kinesis Data Stream is incorrect because there is no Step Scaling feature for Kinesis Data Streams. This is only applicable for EC2.

References:

<https://aws.amazon.com/blogs/big-data/scale-your-amazon-kinesis-stream-capacity-with-updateshardcount/>

<https://aws.amazon.com/kinesis/data-streams/faqs/>

<https://docs.aws.amazon.comstreams/latest/dev/kinesis-using-sdk-java-resharding.html>

[Go back to Q65](#)

Answer to Q66: C

[Go back to Q66](#)

Explanation to Q66

With the event sourcing pattern, instead of updating data stores directly, any events with significance to business logic such as orders being placed, credit inquiries being made, or orders being processed or shipped are added to a durable event log. Because each event record is stored individually, all updates are atomic (indivisible and irreducible). A key characteristic of this pattern is that the application state at any point in time can be rebuilt by simply reprocessing the stored events. Because data is stored as a series of events rather than through direct updates to data stores, various services can replay events from the event store to compute the appropriate state of their respective data stores.

Event sourcing heavily relies on the persistence of events so it can rebuild/replay the state of your application at any given point in time in the past. Among the options given, Amazon Kinesis Data Firehose is the most suitable service to stream data as it provides an ordering of records, as well as the ability to read and/or replay records in the same order.

Hence, the correct answer is the option that says: Configure the first microservice to send data to Amazon Kinesis Data Firehose Stream, then send the event log to an Amazon S3 bucket. Modify the second microservice to fetch data from the Kinesis stream.

The option that says: Configure the first microservice to send data to an Amazon SQS queue, then send the event log to an Amazon S3 bucket. Modify the second microservice to fetch data from the queue is incorrect because although SQS queue can be used as an event source, it does not have the functionality required in building an event store as it is just used to decouple applications by storing messages in the queue as they travel between computers. Amazon Kinesis Data Firehose Stream can preserve the order of records and can also replay the records in the same order which is the key characteristic of an event sourcing application.

The option that says: Configure the first microservice to send data to Amazon SNS topic, then send the event log to an Amazon S3 bucket. Modify the second microservice to fetch data from the topic is incorrect because Amazon SNS is mainly used for sending notifications and not suitable for streaming data.

The option that says: Configure the first microservice to send data to Amazon S3 bucket. Modify the second microservice to fetch data from the bucket is incorrect because in an event sourcing architecture, Amazon S3 is mainly used as a durable storage for event logs and not for streaming data.

References:

<https://d0.awsstatic.com/whitepapers/microservices-on-aws.pdf>

<https://aws.amazon.com/kinesis/data-firehose/?kinesis-blogs.sort-by=item.additionalFields.createdDate&kinesis-blogs.sort-order=desc>

[Go back to Q66](#)

Answer to Q67: A

[Go back to Q67](#)

Explanation to Q67

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Amazon CloudWatch is incorrect because this is primarily used for systems monitoring based on the server metrics. It does not have the capability to track API calls to your AWS resources.

AWS X-Ray is incorrect because this is usually used to debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance. Unlike CloudTrail, it does not record the API calls that were made to your AWS resources.

Amazon API Gateway is incorrect because this is not used for logging each API call to your AWS resources. It is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

Reference:

<https://aws.amazon.com/cloudtrail/>

[Go back to Q67](#)

Answer to Q68: C, E

[Go back to Q68](#)

Explanation to Q68

Application Load Balancers support Weighted Target Groups routing. With this feature, you will be able to do weighted routing of the traffic forwarded by a rule to multiple target groups. This enables various use cases like blue-green, canary and hybrid deployments without the need for multiple load balancers. It even enables zero-downtime migration between on-premises and cloud or between different compute types like EC2 and Lambda.

To divert 50% of the traffic to the new application in AWS and the other 50% to the application, you can also use Route 53 with Weighted routing policy. This will divert the traffic between the on-premises and AWS-hosted application accordingly.

Weighted routing lets you associate multiple resources with a single domain name (techrad.io) or subdomain name (portal.techrad.io) and choose how much traffic is routed to each resource. This can be useful for a variety of purposes, including load balancing and testing new versions of software. You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights.

For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1/256th of the traffic ($1/1+255$), and the other resource gets 255/256ths ($255/1+255$). You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0. When you create a target group in your Application Load Balancer, you specify its target type. This determines the type of target you specify when registering with this target group. You can select the following target

types:
1. instance - The targets are specified by instance ID.
2. ip - The targets are IP addresses.
3. Lambda - The target is a Lambda function.

When the target type is IP, you can specify IP addresses from one of the following CIDR blocks:- 10.0.0.0/8 (RFC 1918)- 100.64.0.0/10 (RFC 6598)- 172.16.0.0/12 (RFC 1918)- 192.168.0.0/16 (RFC 1918)- The subnets of the VPC for the target group.

These supported CIDR blocks enable you to register the following with a target group: ClassicLink instances, instances in a VPC that is peered to the load balancer VPC, AWS resources that are addressable by IP address and port (for example, databases), and on-premises resources linked to AWS through AWS Direct Connect or a VPN connection.

Take note that you can not specify publicly routable IP addresses. If you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance. If you specify targets using IP addresses, you can route traffic to an instance using any private IP address from one or more network interfaces. This enables multiple applications on an instance to use the same port. Each network interface can have its own security group.

Hence, the correct answers are the following options:- 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.- 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.

The option that says: 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 is

incorrect because a Network Load balancer doesn't have Weighted Target Groups to divert the traffic between the on-premises and AWS-hosted application.

The option that says: 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 is incorrect because you cannot divert and proportion the traffic between the on-premises and AWS-hosted application using Route 53 with Failover routing policy. This is primarily used if you want to configure active-passive failover to your application architecture.

The option that says: 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 is incorrect because although you can control the proportion of traffic directed to each endpoint using AWS Global Accelerator by assigning weights across the endpoints, it is still wrong to use a Direct Connect Gateway and an AnyCast IP address since these are not required at all. You can only associate static IP addresses provided by AWS Global Accelerator to regional AWS resources or endpoints, such as Network Load Balancers, Application Load Balancers, EC2 Instances, and Elastic IP addresses.

Take note that a Direct Connect Gateway, per se, doesn't establish a connection from your on-premises network to your Amazon VPCs. It simply enables you to use your AWS Direct Connect connection to connect to two or more VPCs that are in different AWS Regions.

References:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html>

[Go back to Q68](#)

Answer to Q69: A

[Go back to Q69](#)

Explanation to Q69

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues. Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

[Go back to Q69](#)

Answer to Q70: C

[Go back to Q70](#)

Explanation to Q70

The describe-instances command shows the status of the EC2 instances including the recently terminated instances. It also returns a StateReason of why the instance was terminated.

Reference:

<http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>

[Go back to Q70](#)

Answer to Q71: B

[Go back to Q71](#)

Explanation to Q71

Outputs is an optional section of the CloudFormation template that describes the values that are returned whenever you view your stack's properties.

Reference:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html>

<https://aws.amazon.com/cloudformation/>

[Go back to Q71](#)

Answer to Q72: A

[Go back to Q72](#)

Explanation to Q72

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has small, random I/O operations or large, sequential I/O operations.

Since the scenario has workloads with large, sequential I/O operations, we can narrow down our options by selecting HDD volumes, instead of SDD volumes which are more suitable for small, random I/O operations.

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.

Throughput Optimized HDD (st1) volumes, though like Cold HDD (sc1) volumes, are designed to support frequently accessed data.

EBS Provisioned IOPS SSD (io1) is incorrect because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

EBS General Purpose SSD (gp2) is incorrect because although an Amazon EBS General Purpose SSD volume balances price and performance for a wide variety of workloads, it is not suitable for frequently accessed, throughput-intensive workloads. Throughput Optimized HDD is a more suitable option to use than General Purpose SSD. EBS Cold HDD (sc1) is incorrect because although this provides lower cost HDD volume compared to General Purpose SSD, it is much suitable for less frequently accessed workloads.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeType_s.html#EBSVolumeTypes_st1

[Go back to Q72](#)

Answer to Q73: D

[Go back to Q73](#)

Explanation to Q73

NA

[Go back to Q73](#)

Answer to Q74: B

[Go back to Q74](#)

Explanation to Q74

All the APIs created with Amazon API Gateway expose HTTPS endpoints only. Amazon API Gateway does not support unencrypted (HTTP) endpoints. By default, Amazon API Gateway assigns an internal domain to the API that automatically uses the Amazon API Gateway certificate. When configuring your APIs to run under a custom domain name, you can provide your own certificate for the domain.

Reference:

<https://aws.amazon.com/api-gateway/faqs/>

[Go back to Q74](#)

Answer to Q75: A

[Go back to Q75](#)

Explanation to Q75

Failover is automatically handled by Amazon Aurora so that your applications can resume database operations as quickly as possible without manual administrative intervention.

If you have an Amazon Aurora Replica in the same or a different Availability Zone, when failing over, 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. Start-to-finish, failover typically completes within 30 seconds.

If you are running Aurora Serverless and the DB instance or AZ become unavailable, Aurora will automatically recreate the DB instance in a different AZ.

If you do not have an Amazon Aurora Replica (i.e. single instance) and are not running Aurora Serverless, Aurora will attempt to create a new DB Instance in the same Availability Zone as the original instance. This replacement of the original instance is done on a best-effort basis and may not succeed, for example, if there is an issue that is broadly affecting the Availability Zone.

Hence, the correct answer is the option that says: 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.

The options that say: 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 and 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 are incorrect because this will only happen if you are using an Amazon Aurora Replica. In addition, Amazon

Aurora flips the canonical name record (CNAME) and not the A record (IP address) of the instance.

The option that says: 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 is incorrect because Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone and not the other way around.

References:

<https://aws.amazon.com/rds/aurora/faqs/>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html>

[Go back to Q75](#)

Answer to Q76: B

[Go back to Q76](#)

Explanation to Q76

NA

[Go back to Q76](#)

Answer to Q77: A, B, C

[Go back to Q77](#)

Explanation to Q77

The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly.

With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.
2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.
3. If there are multiple instances to terminate based on the above criteria, determine which unprotected instances are closest to the next billing hour. (This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.
4. If there is more than one unprotected instance closest to the next billing hour, choose one of these instances at random.

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-termination-policy>

[Go back to Q77](#)

Answer to Q78: A, D

[Go back to Q78](#)

[Explanation to Q78](#)

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another Amazon S3 storage class. For example: When you know that objects are infrequently accessed, you might transition them to the STANDARD_IA storage class. Or transition your data to the GLACIER storage class in case you want to archive objects that you don't need to access in real time.

In a lifecycle configuration, you can define rules to transition objects from one storage class to another to save on storage costs. When you don't know the access patterns of your objects or your access patterns are changing over time, you can transition the objects to the INTELLIGENT_TIERING storage class for automatic cost savings.

The lifecycle storage class transitions have a constraint when you want to transition from the STANDARD storage classes to either STANDARD_IA or ONEZONE_IA. The following constraints apply:- For larger objects, there is a cost benefit for transitioning to STANDARD_IA or ONEZONE_IA. Amazon S3 does not transition objects that are smaller than 128 KB to the STANDARD_IA or ONEZONE_IA storage classes because it's not cost effective.- Objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD_IA or ONEZONE_IA. For example, you cannot create a lifecycle rule to transition objects to the STANDARD_IA storage class one day after you create them. Amazon S3 doesn't transition objects within the first 30 days because newer objects are often accessed more frequently or deleted sooner than is suitable for STANDARD_IA or ONEZONE_IA storage.- If you are transitioning noncurrent objects (in versioned buckets), you can transition only objects that are at least 30 days noncurrent to STANDARD_IA or ONEZONE_IA storage.

Since there is a time constraint in transitioning objects in S3, you can only change the storage class of your objects from S3 Standard storage class to STANDARD_IA or ONEZONE_IA storage after 30 days. This limitation does not apply on INTELLIGENT_TIERING, GLACIER, and DEEP_ARCHIVE storage class.

In addition, the requirement says that the media assets should be fetched in a matter of minutes for a surprise annual data audit. This means that the retrieval will only happen once a year. You can use expedited retrievals in Glacier which will allow you to quickly access your data (within 15 minutes) when occasional urgent requests for a subset of archives are required.

In this scenario, you can set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days or alternatively, you can directly transition your data to Glacier after one week (7 days). Hence, the following are the correct answers:- Set a lifecycle policy in the bucket to transition the data from Standard storage class to Glacier after one week (7 days).- Set a lifecycle policy in the bucket to transition to S3 - Standard IA after 30 days.

Setting a lifecycle policy in the bucket to transition the data to S3 - Standard IA storage class after one week (7 days) and setting a lifecycle policy in the bucket to transition the data to S3 - One Zone-Infrequent Access storage class after one week (7 days) are both incorrect because there is a constraint in S3 that objects must be stored at least 30 days in the current storage class before you can transition them to STANDARD_IA or ONEZONE_IA. You cannot create a lifecycle rule to transition objects to either STANDARD_IA or ONEZONE_IA storage class 7 days after you create them because you can only do this after the 30-day period has elapsed. Hence, these options are incorrect.

Setting a lifecycle policy in the bucket to transition the data to S3 Glacier Deep Archive storage class after one week (7 days) is incorrect because although DEEP_ARCHIVE storage class provides the most cost-effective storage option, it does not have the ability to do expedited retrievals, unlike Glacier. If the surprise annual data audit happens, it may take several hours before you can retrieve your data.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/restoring-objects.html>

<https://aws.amazon.com/s3/storage-classes/>

[Go back to Q78](#)

Answer to Q79: B

[Go back to Q79](#)

Explanation to Q79

NA

[Go back to Q79](#)

Answer to Q80: D

[Go back to Q80](#)

Explanation to Q80

Glacier is a cost-effective archival solution for large amounts of data. Bulk retrievals are S3 Glaciers lowest-cost retrieval option, enabling you to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5–12 hours. You can specify an absolute or relative time period (including 0 days) after which the specified Amazon S3 objects should be transitioned to Amazon Glacier.

Hence, the correct answer is the option that says: Upload the data to S3 and set a lifecycle policy to transition data to Glacier after 0 days.

Glacier has a management console that you can use to create and delete vaults. However, you cannot directly upload archives to Glacier by using the management console. To upload data such as photos, videos, and

other documents, you must either use the AWS CLI or write code to make requests by using either the REST API directly or by using the AWS SDKs.

Take note that uploading data to the S3 Console and setting its storage class of "Glacier" is a different story as the proper way to upload data to Glacier is still via its API or CLI. In this way, you can set up your vaults and configure your retrieval options. If you uploaded your data using the S3 console, then it will be managed via S3 even though it is internally using a Glacier storage class.

Uploading the data to S3 then using a lifecycle policy to transfer data to S3-IA is incorrect because using Glacier would be a more cost-effective solution than using S3-IA. Since the required retrieval period should not exceed more than a day, Glacier would be the best choice.

Uploading the data to Amazon FSx for Windows File Server using the Server Message Block (SMB) protocol is incorrect because this option costs more than Amazon Glacier, which is more suitable for storing infrequently accessed data. Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Uploading the data to S3 then using a lifecycle policy to transfer data to S3 One Zone-IA is incorrect because with S3 One Zone-IA, the data will only be stored in a single availability zone and thus, this storage solution is not durable. It also costs more compared to Glacier.

References:

<https://aws.amazon.com/glacier/faqs/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-an-archive.html>

[Go back to Q80](#)

Answer to Q81: D

[Go back to Q81](#)

Explanation to Q81

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

Using CloudTrail and configuring the destination Amazon Glacier archive to use Server-Side Encryption (SSE) is incorrect because CloudTrail stores the log files to S3 and not in Glacier. Take note that by default, CloudTrail event log files are already encrypted using Amazon S3 server-side encryption (SSE). Using CloudTrail and configuring the destination S3 bucket to use Server-Side Encryption (SSE) is incorrect because CloudTrail event log files are already encrypted using the Amazon S3 server-side encryption (SSE) which is why you do not have to do this anymore.

Use CloudTrail and configure the destination S3 bucket to use Server Side Encryption (SSE) with AES-128 encryption algorithm is incorrect because CloudTrail event log files are already encrypted using the Amazon S3 server-side encryption (SSE) by default. Additionally, SSE-S3 only uses the AES-256 encryption algorithm and not the AES-128.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

<https://aws.amazon.com/blogs/aws/category/cloud-trail/>

[Go back to Q81](#)

Answer to Q82: A

[Go back to Q82](#)

Explanation to Q82

In this scenario, the technology company is looking for a storage service that will enable their analytics application to frequently access the latest data subsets and not the entire data set because it was mentioned that the old data are rarely being used. This requirement can be fulfilled by setting up a Cached Volume Gateway in AWS Storage Gateway.

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to frequently accessed data. You can create storage volumes up to 32 TiB in size and afterwards, attach these volumes as iSCSI devices to your on-premises application servers. When you write to these volumes, your gateway stores the data in Amazon S3. It retains the recently read data in your on-premises storage gateway's cache and uploads buffer storage. Cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB). In the cached volumes solution, AWS Storage Gateway stores all you're on-premises application data in a storage volume in Amazon S3.

Hence, the correct answer is Cached Volume Gateway.

Stored Volume Gateway is incorrect because the requirement is to provide low latency access to the frequently accessed data subsets locally. Stored Volume Gateway is used if you need low-latency access to your entire dataset.

Tape Gateway is incorrect because this is just a cost-effective, durable, long-term offsite alternative for data archiving, which is not needed in this scenario.

File Gateway is incorrect because this does not provide you the required low-latency access to the frequently accessed data that the on-site analytics application needs.

References:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html#volume-gateway-concepts>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

[Go back to Q82](#)

Answer to Q83: D

[Go back to Q83](#)

Explanation to Q83

Amazon SQS automatically deletes messages that have been in a queue for more than the maximum message retention period. The default message retention period is 4 days. Since the queue is configured to the default settings and the batch job application only processes the messages once a week, the messages that are in the queue for more than 4 days are deleted. This is the root cause of the issue. To fix this, you can increase the

message retention period to a maximum of 14 days using the SetQueueAttributes action.

References:

<https://aws.amazon.com/sqs/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

[Go back to Q83](#)

Answer to Q84: A

[Go back to Q84](#)

Explanation to Q84

NA

[Go back to Q84](#)

Answer to Q85: D

[Go back to Q85](#)

Explanation to Q85

In this scenario, a legacy batch application which has steady-state workloads requires a relational MySQL database. The EBS volume that you should use has to handle a maximum of 450 GB of data and can also be used as the system boot volume for your EC2 instance. Since HDD volumes cannot be used as a bootable volume, we can narrow down our options by selecting SSD volumes. In addition, SSD volumes are more suitable for transactional database workloads.

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time. AWS designs gp2 volumes to deliver the provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

Amazon EBS Provisioned IOPS SSD (io1) is incorrect because this is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

Amazon EBS Throughput Optimized HDD (st1) is incorrect because this is primarily used for frequently accessed, throughput-intensive workloads. Although it is a low-cost HDD volume, it cannot be used as a system boot volume.

Amazon EBS Cold HDD (sc1) is incorrect because although Amazon EBS Cold HDD provides lower cost HDD volume compared to General Purpose SSD, it cannot be used as a system boot volume.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2

[Go back to Q85](#)

Answer to Q86: C

[Go back to Q86](#)

Explanation to Q86

A load balancer takes requests from clients and distributes them across the EC2 instances that are registered with the load balancer. You can create a

load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted. If the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.

If your load balancer uses an encrypted connection to communicate with the instances, you can optionally enable authentication of the instances. This ensures that the load balancer communicates with an instance only if its public key matches the key that you specified to the load balancer for this purpose.

The type of ELB that is mentioned in this scenario is an Application Elastic Load Balancer. This is used if you want a flexible feature set for your web applications with HTTP and HTTPS traffic. Conversely, it only allows 2 types of health check: HTTP and HTTPS.

Hence, the correct answer is: HTTP or HTTPS health check.

ICMP health check and FTP health check are incorrect as these are not supported.

TCP health check is incorrect. A TCP health check is only offered in Network Load Balancers and Classic Load Balancers.

References:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>

[Go back to Q86](#)

Answer to Q87: A, B

[Go back to Q87](#)

Explanation to Q87

In Amazon Kinesis, the producers continually push data to Kinesis Data Streams and the consumers process the data in real time. Consumers (such as a custom application running on Amazon EC2, or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3. Hence, Amazon S3 and Amazon Redshift are the correct answers.

Glacier Select is incorrect because this is not a storage service. It is primarily used to run queries directly on data stored in Amazon Glacier, retrieving only the data you need out of your archives to use for analytics.

AWS Glue is incorrect because this is not a storage service. It is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

Amazon Athena is incorrect because this is just an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. It is not a storage service where you can store the results processed by the consumers.

Reference:

<http://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

[Go back to Q87](#)

Answer to Q88: D

[Go back to Q88](#)

Explanation to Q88

NA

[Go back to Q88](#)

Answer to Q89: D

[Go back to Q89](#)

Explanation to Q89

AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. It inspects your AWS environment and makes recommendations for saving money, improving system performance and reliability, or closing security gaps.

Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Cost Optimization recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill.

Security identification of security settings that could make your AWS solution less secure.

Fault Tolerance recommendations that help increase the resiliency of your AWS solution by highlighting redundancy shortfalls, current service limits, and over-utilized resources.

Performance recommendations that can help to improve the speed and responsiveness of your applications.

Service Limits recommendations that will tell you when service usage is more than 80% of the service limit.

Hence, the correct answer in this scenario is AWS Trusted Advisor.

AWS Cost Explorer is incorrect because this is just a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. It has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

AWS Budgets is incorrect because it simply gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define.

Amazon Inspector is incorrect because it is just an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

References:

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/faqs/>

[Go back to Q89](#)

Answer to Q90: B

[Go back to Q90](#)

Explanation to Q90

The EC2 instances in an Auto Scaling group have a path, or lifecycle, that differs from that of other EC2 instances. The lifecycle starts when the Auto Scaling group launches an instance and puts it into service. The lifecycle ends when you terminate the instance, or the Auto Scaling group takes the instance out of service and terminates it.

You can add a lifecycle hook to your Auto Scaling group so that you can perform custom actions when instances launch or terminate.

When Amazon EC2 Auto Scaling responds to a scale out event, it launches one or more instances. These instances start in the Pending state. If you added an `autoscaling:EC2_INSTANCE_LAUNCHING` lifecycle hook to your Auto Scaling group, the instances move from the Pending state to the Pending:Wait state. After you complete the lifecycle action, the instances enter the Pending:Proceed state. When the instances are fully configured, they are attached to the Auto Scaling group and they enter the InService state.

When Amazon EC2 Auto Scaling responds to a scale in event, it terminates one or more instances. These instances are detached from the Auto Scaling group and enter the Terminating state. If you added an `autoscaling:EC2_INSTANCE_TERMINATING` lifecycle hook to your Auto Scaling group, the instances move from the Terminating state to the Terminating:Wait state. After you complete the lifecycle action, the instances enter the Terminating:Proceed state. When the instances are fully terminated, they enter the Terminated state.

Using CloudWatch agent is the most suitable tool to use to collect the logs. The unified CloudWatch agent enables you to do the following:- Collect more system-level metrics from Amazon EC2 instances across operating systems. The metrics can include in-guest metrics, in addition to the metrics for EC2 instances. The additional metrics that can be collected are listed in Metrics Collected by the CloudWatch Agent.- Collect system-level metrics from on-premises servers. These can include servers in a hybrid

environment as well as servers not managed by AWS.- Retrieve custom metrics from your applications or services using the StatsD and collectd protocols. StatsD is supported on both Linux servers and servers running Windows Server. collectd is supported only on Linux servers.- Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.

You can store and view the metrics that you collect with the CloudWatch agent in CloudWatch just as you can with any other CloudWatch metrics. The default namespace for metrics collected by the CloudWatch agent is CWAgent, although you can specify a different namespace when you configure the agent.

Hence, the correct answer is: 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.

The option that says: Add a lifecycle hook to your Auto Scaling group to move instances in the Terminating state to 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 is incorrect because the Pending:Wait state refers to the scale-out action in Amazon EC2 Auto Scaling and not for scale-in or for terminating the instances.

The option that says: 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 is incorrect because using AWS Step Functions is inappropriate in collecting the logs from your EC2 instances. You should use a CloudWatch agent instead.

The option that says: 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 is incorrect because although this solution could work, it entails a lot of effort to write a custom script that the AWS Systems Manager Run Command will run. Remember that the scenario asks for a solution that you can implement with the least amount of effort. This solution can be simplified by automatically uploading the logs using a CloudWatch Agent. You must use the EC2 Instance-terminate Lifecycle Action event instead.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroupLifecycle.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/cloud-watch-events.html#terminate-successful>

<https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-delay-termination/>

[Go back to Q90](#)

Answer to Q91: B

[Go back to Q91](#)

Explanation to Q91

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases.

AWS Database Migration Service can migrate your data to and from most of the widely used commercial and open source databases. It supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora. Migrations can be from on-premises databases to Amazon RDS or Amazon EC2, databases running on EC2 to RDS, or vice versa, as well as from one RDS database to another RDS database. It can also move data between SQL, NoSQL, and text-based targets.

In heterogeneous database migrations the source and target databases engines are different, like in the case of Oracle to Amazon Aurora, Oracle to PostgreSQL, or Microsoft SQL Server to MySQL migrations. In this case, the schema structure, data types, and database code of source and target databases can be quite different, requiring a schema and code transformation before the data migration starts. That makes heterogeneous migrations a two-step process.

First use the AWS Schema Conversion Tool to convert the source schema and 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. All the required data type conversions will automatically be done by the AWS Database Migration Service during the migration. The source database can be in your own premises outside of

AWS, running on an Amazon EC2 instance, or it can be an Amazon RDS database. The target can be a database in Amazon EC2 or Amazon RDS.

The option that says: 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 is incorrect because Launch templates are primarily used in EC2 to enable you to store launch parameters so that you do not have to specify them every time you launch an instance.

The option that says: 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 is incorrect because Amazon Neptune is a fully-managed graph database service and not a suitable service to use to convert the source schema. AWS Batch is not a database migration service and hence, it is not suitable to be used in this scenario. You should use the AWS Schema Conversion Tool and AWS Database Migration Service instead.

The option that says: Heterogeneous database migration is not supported in AWS. You must transform your database first to PostgreSQL and then migrate it to RDS is incorrect because heterogeneous database migration is supported in AWS using the Database Migration Service.

References:

<https://aws.amazon.com/dms/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html>

<https://aws.amazon.com/batch/>

[Go back to Q91](#)

Answer to Q92: B

[Go back to Q92](#)

Explanation to Q92

For this scenario, the best way to achieve the required solution is to use a combination of Tags and IAM policies. You can define the tags on the UAT and production EC2 instances and add a condition to the IAM policy which allows access to specific tags.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type you can quickly identify a specific resource based on the tags you've assigned to it.

By default, IAM users don't have permission to create or modify Amazon EC2 resources, or perform tasks using the Amazon EC2 API. (This means that they also can't do so using the Amazon EC2 console or CLI.) To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant IAM users permission to use the specific resources and API actions they'll need, and then attach those policies to the IAM users or groups that require those permissions.

Hence, the correct answer is: Define the tags on the UAT and production servers and add a condition to the IAM policy which allows access to specific tags.

The option that says: Launch the UAT and production EC2 instances in separate VPC's connected by VPC peering is incorrect because these are just network changes to your cloud architecture and doesn't have any effect on the security permissions of your users to access your EC2 instances.

The option that says: Provide permissions to the users via the AWS Resource Access Manager (RAM) service to only access EC2 instances that

are used for production or development is incorrect because the AWS Resource Access Manager (RAM) is primarily used to securely share your resources across AWS accounts or within your Organization and not on a single AWS account. You also must set up a custom IAM Policy in order for this to work.

The option that says: Launch the UAT and production instances in different Availability Zones and use Multi Factor Authentication is incorrect because placing the EC2 instances to different AZs will only improve the availability of the systems but won't have any significance in terms of security. You must set up an IAM Policy that allows access to EC2 instances based on their tags. In addition, a Multi-Factor Authentication is not a suitable security feature to be implemented for this scenario.

References:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-for-amazon-ec2.html>

[Go back to Q92](#)

Answer to Q93: A

[Go back to Q93](#)

Explanation to Q93

The term "fully managed" means that Amazon will manage the underlying infrastructure of the service hence, you don't need an additional human resource to support or maintain the service. Therefore, Amazon DynamoDB is the right answer. Remember that Amazon RDS is a managed service but not "fully managed" as you still have the option to maintain and configure the underlying server of the database.

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

Amazon Neptune is incorrect because this is primarily used as a graph database.

Amazon Aurora is incorrect because this is a relational database and not a NoSQL database.

SimpleDB is incorrect because although SimpleDB is also a highly available and scalable NoSQL database, it has a limit on the request capacity or storage size for a given table, unlike DynamoDB.

Reference:

<https://aws.amazon.com/dynamodb/>

[Go back to Q93](#)

Answer to Q94: A, D, E

[Go back to Q94](#)

Explanation to Q94

In order for you to access your EC2 instance from the Internet, you need to have:- An Internet Gateway (IGW) attached to the VPC.- A route entry to the Internet gateway in the Route table of the VPC.- A Public IP address attached to the EC2 instance.

A Private IP address attached to the EC2 instance is incorrect as you only use a Private IP inside your VPC. A Private Elastic IP address attached to the EC2 instance is incorrect as an Elastic IP Address is a public IPv4 address, not private. It is reachable from the Internet and is designed for dynamic cloud computing.

A VPN Peering connection is incorrect as you only use VPC Peering to connect two VPCs.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario_1.html

[Go back to Q94](#)

Answer to Q95: B

[Go back to Q95](#)

Explanation to Q95

By using Cached volumes, you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally in your on-premises network. Cached volumes offer substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data. This is the best solution for this scenario.

Using a fleet of EC2 instances with EBS volumes to store the commonly used data is incorrect because an EC2 instance is not a storage service and it does not provide the required durability and scalability.

Using both ElastiCache and S3 for frequently accessed data is incorrect as this is not efficient. Moreover, the question explicitly said that the

frequently accessed data should be stored locally on their on-premises server and not on AWS.

Using Amazon Glacier is incorrect as this is mainly used for data archiving.

Reference:

<https://aws.amazon.com/storagegateway/faqs/>

[Go back to Q95](#)

Answer to Q96: C

[Go back to Q96](#)

Explanation to Q96

Amazon S3 now provides increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which can save significant processing time for no additional charge. Each S3 prefix can support these request rates, making it simple to increase performance significantly.

Applications running on Amazon S3 today will enjoy this performance improvement with no changes, and customers building new applications on S3 do not have to make any application customizations to achieve this performance. Amazon S3's support for parallel requests means you can scale your S3 performance by the factor of your compute cluster, without making any customizations to your application. Performance scales per prefix, so you can use as many prefixes as you need in parallel to achieve the required throughput. There are no limits to the number of prefixes.

This S3 request rate performance increase removes any previous guidance to randomize object prefixes to achieve faster performance. That means you can now use logical or sequential naming patterns in S3 object naming

without any performance implications. This improvement is now available in all AWS Regions.

Using Byte-Range Fetches to retrieve multiple ranges of an object data per GET request is incorrect because although a Byte-Range Fetch helps you achieve higher aggregate throughput, Amazon S3 does not support retrieving multiple ranges of data per GET request. Using the Range HTTP header in a GET Object request, you can fetch a byte-range from an object, transferring only the specified portion. You can use concurrent connections to Amazon S3 to fetch different byte ranges from within the same object. Fetching smaller ranges of a large object also allows your application to improve retry times when requests are interrupted.

Adding a random prefix to the key names is incorrect. Adding a random prefix is not required in this scenario because S3 can now scale automatically to adjust performance. You do not need to add a random prefix anymore for this purpose since S3 has increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which covers the workload in the scenario.

Using a predictable naming scheme in the key names such as sequential numbers or date time sequences is incorrect because Amazon S3 already maintains an index of object key names in each AWS region. S3 stores key names in alphabetical order. The key name dictates which partition the key is stored in. Using a sequential prefix increases the likelihood that Amazon S3 will target a specific partition for many your keys, overwhelming the I/O capacity of the partition.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html>

<https://d1.awsstatic.com/whitepapers/AmazonS3BestPractices.pdf>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/GettingObjectsUsingAPIs.html>

[Go back to Q96](#)

Answer to Q97: C

[Go back to Q97](#)

Explanation to Q97

The AWS Management Console is the web interface used to manage your AWS resources using your web browser. To access this, your users should have a password that they can use to login to the web console.

Providing the system administrators, the secret access key and access key id is incorrect as these are used to trigger AWS API calls.

Enabling multi-factor authentication on their accounts and defining a password policy is incorrect because the multi-factor authentication and a password policy are just additional security measures for the IAM user, but these won't enable them to access the AWS Management Console.

Adding the administrators to the Security Group is incorrect as you can't add an IAM user to a security group. Remember that a security group is primarily used for EC2 instances, and not for IAM.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_how-users-sign-in.html

[Go back to Q97](#)

Answer to Q98: D

[Go back to Q98](#)

Explanation to Q98

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

Reference:

<https://aws.amazon.com/opsworks/>

[Go back to Q98](#)

Answer to Q99: A

[Go back to Q99](#)

Explanation to Q99

In this scenario, one of the Availability Zones is not properly added to the Elastic load balancer. Hence, that Availability Zone is not receiving any traffic.

You can set up your load balancer in EC2-Classic to distribute incoming requests across EC2 instances in a single Availability Zone or multiple Availability Zones. First, launch EC2 instances in all the Availability Zones that you plan to use. Next, register these instances with your load balancer. Finally, add the Availability Zones to your load balancer. After you add an Availability Zone, the load balancer starts routing requests to the registered instances in that Availability Zone. Note that you can modify the Availability Zones for your load balancer at any time.

By default, the load balancer routes requests evenly across its Availability Zones. To route requests evenly across the registered instances in the Availability Zones, enable cross-zone load balancing.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html>

[Go back to Q99](#)

Answer to Q100: C

[Go back to Q100](#)

Explanation to Q100

In this scenario, the company has an existing IAM role hence you don't need to create a new one. IAM roles are global service that are available to all regions hence, all you must do is assign the existing IAM role to the instance in the new region.

The option that says: In the new Region, create a new IAM role and associated policies then assign it to the new instance is incorrect because you don't need to create another IAM role - there is already an existing one.

Duplicating the IAM role and associated policies to the new region and attaching it to the instances is incorrect as you don't need duplicate IAM roles for each region. One IAM role suffices for the instances on two regions.

Creating an Amazon Machine Image (AMI) of the instance and copying it to the new region is incorrect because creating an AMI image does not affect the IAM role of the instance.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

[Go back to Q100](#)

Answer to Q101: D

[Go back to Q101](#)

Explanation to Q101

You manage your DB engine configuration using parameters in a DB parameter group. DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances.

Reference:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html

[Go back to Q101](#)

Answer to Q102: B

[Go back to Q102](#)

Explanation to Q102

Take note that your VPC lives within a larger AWS network and the services, such as S3, DynamoDB, RDS and many others, are located outside of your VPC, but still within the AWS network. By default, the connection that your VPC uses to connect to your S3 bucket or any other service traverses the public Internet via your Internet Gateway.

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

There are two types of VPC endpoints: interface endpoints and gateway endpoints. You must create the type of VPC endpoint required by the supported service.

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service. It is important to note that for Amazon S3 and DynamoDB service, you must create a gateway endpoint and then use an interface endpoint for other services.

Changing the web architecture to access the financial data in your S3 bucket through a VPN connection is incorrect because a VPN connection still goes through the public Internet. You have to use a VPC Endpoint in this scenario and not VPN, to privately connect your VPC to supported AWS services such as S3. Changing the web architecture to access the financial data hosted in your S3 bucket by creating a custom VPC endpoint service is incorrect because a "VPC endpoint service" is quite different from a "VPC endpoint".

With VPC endpoint service, you are the service provider where you can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint.

Changing the web architecture to access the financial data in S3 through an interface VPC endpoint, which is powered by AWS PrivateLink is incorrect

because although you are correctly using a VPC Endpoint to satisfy the requirement, you chose a wrong type of VPC Endpoint. Remember that for S3 and DynamoDB service, you must use a Gateway VPC Endpoint and not an Interface VPC Endpoint.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

[Go back to Q102](#)

Answer to Q103: C

[Go back to Q103](#)

Explanation to Q103

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.

An instance store consists of one or more instance store volumes exposed as block devices. The size of an instance store as well as the number of devices available varies by instance type. While an instance store is dedicated to an instance, the disk subsystem is shared among instances on a host computer.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or

unintentionally), data in the instance store persists. However, data in the instance store is lost under the following circumstances:- The underlying disk drive fails- The instance stops- The instance terminates.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

[Go back to Q103](#)

Answer to Q104: D

[Go back to Q104](#)

Explanation to Q104

Since the application is scaling up and down multiple times within the hour, the issue lies on the cooldown period of the Auto Scaling group. The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities. When you manually scale your Auto Scaling group, the default is not to wait for the cooldown period, but you can override the default and honor the cooldown period. If an instance becomes unhealthy, the Auto Scaling group does not wait for the cooldown period to complete before replacing the unhealthy instance.

Reference:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-scale-based-on-demand.html>

[Go back to Q104](#)

Answer to Q105: C

[Go back to Q105](#)

Explanation to Q105

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast-distributed storage. The underlying storage grows automatically as needed, up to 64 tebibytes (TiB). Aurora also automates and standardizes database clustering and replication, which are typically among the most challenging aspects of database configuration and administration.

For Amazon RDS MariaDB DB instances, the maximum provisioned storage limit constrains the size of a table to a maximum size of 64 TB when using InnoDB file-per-table tablespaces. This limit also constrains the system tablespace to a maximum size of 16 TB. InnoDB file-per-table tablespaces (with tables each in their own tablespace) is set by default for Amazon RDS MariaDB DB instances.

Hence, the correct answer is Amazon Aurora.

Amazon Redshift is incorrect because this is primarily used for OLAP applications and not for OLTP. Moreover, it doesn't scale automatically to handle the exponential growth of the database.

Amazon DynamoDB is incorrect. Although you can use this to have an ACID-compliant database, it is not capable of handling complex queries and highly transactional (OLTP) workloads.

Amazon RDS is incorrect. Although this service can host an ACID-compliant relational database that can handle complex queries and transactional (OLTP) workloads, it is still not scalable to handle the growth of the database. Amazon Aurora is the better choice as its underlying storage can grow automatically as needed.

References:

<https://aws.amazon.com/rds/aurora/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQltoNoSQL.html>

<https://aws.amazon.com/nosql/>

[Go back to Q105](#)

Answer to Q106: D

[Go back to Q106](#)

Explanation to Q106

Route 53's DNS implementation connects user requests to infrastructure running inside (and outside) of Amazon Web Services (AWS). For example, if you have multiple web servers running on EC2 instances behind an Elastic Load Balancing load balancer, Route 53 will route all traffic

addressed to your website (e.g. www.techrad.io) to the load balancer DNS name (e.g. elbtechradio123.elb.amazonaws.com). Additionally, Route 53 supports the alias resource record set, which lets you map your zone apex (e.g. techrad.io) DNS name to your load balancer DNS name. IP addresses associated with Elastic Load Balancing can change at any time due to scaling or software updates. Route 53 responds to each request for an Alias resource record set with one IP address for the load balancer.

Creating an A record pointing to the IP address of the load balancer is incorrect. You should be using an Alias record pointing to the DNS name of the load balancer since the IP address of the load balancer can change at any time.

Creating a CNAME record pointing to the load balancer DNS name and creating an alias for CNAME record to the load balancer DNS name are incorrect because CNAME records cannot be created for your zone apex. You should create an alias record at the top node of a DNS namespace which is also known as the zone apex. For example, if you register the DNS name techrad.io, the zone apex is techrad.io. You can't create a CNAME record directly for techrad.io, but you can create an alias record for techrad.io that routes traffic to www.techrad.io.

References:

<http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

[Go back to Q106](#)

Answer to Q107: C

[Go back to Q107](#)

Explanation to Q107

Amazon ECS lets you run batch workloads with managed or custom schedulers on Amazon EC2 On-Demand Instances, Reserved Instances, or Spot Instances. You can launch a combination of EC2 instances to set up a cost-effective architecture depending on your workload. You can launch Reserved EC2 instances to process the mission-critical data and Spot EC2 instances for processing non-essential batch jobs.

There are two different charge models for Amazon Elastic Container Service (ECS): Fargate Launch Type Model and EC2 Launch Type Model. With Fargate, you pay for vCPU and memory resources that your containerized application requests while for EC2 launch type model, there is no additional charge. You pay for AWS resources (e.g. EC2 instances or EBS volumes) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

In this scenario, the most cost-effective solution is to 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. You can use Scheduled Reserved Instances (Scheduled Instances) which enables you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. This will ensure that you have an uninterrupted compute capacity to process your mission-critical batch jobs.

Hence, the correct answer is the option that says: 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.

Using ECS as the container management service then setting up Reserved EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because processing the non-essential batch jobs can be

handled much cheaper by using Spot EC2 instances instead of Reserved Instances.

Using ECS as the container management service then setting up On-Demand EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because an On-Demand instance costs more compared to Reserved and Spot EC2 instances. Processing the non-essential batch jobs can be handled much cheaper by using Spot EC2 instances instead of On-Demand instances.

Using ECS as the container management service then setting up Spot EC2 Instances for processing both mission-critical and non-essential batch jobs is incorrect because although this set up provides the cheapest solution among other options, it will not be able to meet the required workload. Using Spot instances to process mission-critical workloads is not suitable since these types of instances can be terminated by AWS at any time, which can affect critical processing.

References:

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcom e.html>

<https://aws.amazon.com/ec2/spot/containers-for-less/get-started/>

[Go back to Q107](#)

Answer to Q108: B

[Go back to Q108](#)

Explanation to Q108

NA

[Go back to Q108](#)

Answer to Q109: B

[Go back to Q109](#)

Explanation to Q109

You can use Run Command from the console to configure instances without having to login to each instance.

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.

Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>

[Go back to Q109](#)

Answer to Q110: D

[Go back to Q110](#)

Explanation to Q110

In this scenario, you need a service that can collect, process, and analyze data in real-time hence, the right service to use here is Amazon Kinesis.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.

With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

All other options are incorrect since these services do not have real-time processing capability, unlike Amazon Kinesis.

Reference:

<https://aws.amazon.com/kinesis/> Check out this Amazon Kinesis

[Go back to Q110](#)

Answer to Q111: B

[Go back to Q111](#)

Explanation to Q111

An edge location helps deliver high availability, scalability, and performance of your application for all your customers from anywhere in the world. This is used by other services such as Lambda and Amazon CloudFront.

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content

with low latency and high data transfer speeds. CloudFront delivers your files to end-users using a global network of edge locations.

Bastion Hosts is incorrect because a bastion host is not part of the AWS Global Infrastructure. It is just a host computer or a "jump server" used to allow SSH access to your EC2 instances from an outside network.

Hypervisor is incorrect because this is just a computer software, firmware or hardware that creates and runs virtual machines. This technology relates to EC2 instances, but it is not part of the AWS Global Infrastructure.

VPC Endpoint is incorrect because this is not part of the AWS Global Infrastructure and is just used to privately connect your VPC to other AWS services and endpoint services.

References:

<https://aws.amazon.com/cloudfront/>

<https://aws.amazon.com/about-aws/global-infrastructure/>

[Go back to Q111](#)

Answer to Q112: A, D

[Go back to Q112](#)

Explanation to Q112

Amazon EC2 Auto Scaling provides you with an option to enable automatic scaling for one or more EC2 instances by attaching them to your existing Auto Scaling group. After the instances are attached, they become a part of the Auto Scaling group.

The instance that you want to attach must meet the following criteria:- The instance is in the running state.- The AMI used to launch the instance must

still exist.- The instance is not a member of another Auto Scaling group.- The instance is launched into one of the Availability Zones defined in your Auto Scaling group.- If the Auto Scaling group has an attached load balancer, the instance and the load balancer must both be in EC2-Classic or the same VPC. If the Auto Scaling group has an attached target group, the instance and the load balancer must both be in the same VPC.

Based on the above criteria, the following are the correct answers among the given options:- You have to ensure that the AMI used to launch the instance still exists.- You have to ensure that the instance is launched in one of the Availability Zones defined in your Auto Scaling group.

The option that says: You must stop the instance first is incorrect because you can directly add a running EC2 instance to an Auto Scaling group without stopping it.

The option that says: You must ensure that the AMI used to launch the instance no longer exists is incorrect because it should be the other way around. The AMI used to launch the instance should still exist.

The option that says: You must ensure that the instance is in a different Availability Zone as the Auto Scaling group is incorrect because the instance should be launched in one of the Availability Zones defined in your Auto Scaling group.

References:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/attach-instance-asg.html>

https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html

[Go back to Q112](#)

Answer to Q113: C, E

[Go back to Q113](#)

Explanation to Q113

Amazon EBS encryption offers seamless encryption of EBS data volumes, boot volumes, and snapshots, eliminating the need to build and maintain a secure key management infrastructure. EBS encryption enables data at rest security by encrypting your data using Amazon-managed keys, or keys you create and manage using the AWS Key Management Service (KMS). The encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.

Hence, the correct answers are: using your own keys in AWS Key Management Service (KMS) and using Amazon-managed keys in AWS Key Management Service (KMS). Using S3 Server-Side Encryption and using S3 Client-Side Encryption are both incorrect as these relate only to S3. Using a password stored in CloudHSM is incorrect as you only store keys in CloudHSM and not passwords.

Using the SSL certificates provided by the AWS Certificate Manager (ACM) is incorrect as ACM only provides SSL certificates and not data encryption of EBS Volumes.

Reference:

<https://aws.amazon.com/ebs/faqs/>

[Go back to Q113](#)

Answer to Q114: A

[Go back to Q114](#)

Explanation to Q114

Direct Connect creates a direct, private connection from your on-premises data center to AWS, letting you establish a 1-gigabit or 10-gigabit dedicated network connection using Ethernet fiber-optic cable.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/connect-vpc/>

[Go back to Q114](#)

Answer to Q115: B

[Go back to Q115](#)

Explanation to Q115

Since the security group is properly configured, the issue may be caused by a wrong health check configuration in the Target Group. Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

[Go back to Q115](#)

Answer to Q116: A

[Go back to Q116](#)

Explanation to Q116

In this question, the keyword is distributed session data management.

Sticky session feature of the Classic Load Balancer can also provide session management, however, take note that this feature has its limitations such as, in the event of a failure, you are likely to lose the sessions that were resident on the failed node. If the number of your web servers change when your Auto Scaling kicks in, it's possible that the traffic may be unequally spread across the web servers as active sessions may exist on servers. If not mitigated properly, this can hinder the scalability of your applications. Hence, sticky session is not scalable or "distributed" as compared with ElastiCache.

You can manage HTTP session data from the web servers using an In-Memory Key/Value store such as Redis and Memcached. Redis is an open source, in-memory data structure store used as a database, cache, and message broker. Memcached is an in-memory key-value store for small arbitrary data (strings, objects) from results of database calls, API calls, or page rendering.

In AWS, you can use Amazon ElastiCache which offers fully managed Redis and Memcached service to manage and store session data for your web applications.

Setting up an AWS Systems Manager Session Manager is incorrect because the Session Manager is simply a capability that lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. This does not act as a distributed session data management.

Enabling the sticky session feature in the Classic Load Balancer is incorrect because although you can use this to manage your session data, it is not a "distributed" solution compared to ElastiCache.

Using the GetSessionToken action in AWS STS for session management is incorrect because GetSessionToken is just one of the available actions in STS which returns a set of temporary credentials for an AWS account or IAM user. This is not used for distributed session data management

References:

<https://aws.amazon.com/caching/session-management/>
<https://aws.amazon.com/elasticache/>

[Go back to Q116](#)

Answer to Q117: A

[Go back to Q117](#)

Explanation to Q117

The visibility timeout is a period during which Amazon SQS prevents other consuming components from receiving and processing a message. When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.

Immediately after the message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period during which Amazon SQS prevents other

consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The maximum is 12 hours.

References:

<https://aws.amazon.com/sqs/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

[Go back to Q117](#)

Answer to Q118: A, D

[Go back to Q118](#)

Explanation to Q118

If you want to allow or block web requests based on the country that the requests originate from, create one or more geo match conditions. A geo match condition lists country that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those countries.

You can use geo match conditions with other AWS WAF Classic conditions or rules to build sophisticated filtering. For example, if you want to block certain countries but still allow specific IP addresses from that country, you could create a rule containing a geo match condition and an IP match condition. Configure the rule to block requests that originate from that country and do not match the approved IP addresses. As another example, if you want to prioritize resources for users in a country, you could include a geo match condition in two different rate-based rules. Set a higher rate limit for users in the preferred country and set a lower rate limit for all other users.

If you are using the CloudFront geo restriction feature to block a country from accessing your content, any request from that country is blocked and is not forwarded to AWS WAF Classic. So, if you want to allow or block requests based on geography plus other AWS WAF Classic conditions, you should not use the CloudFront geo restriction feature. Instead, you should use an AWS WAF Classic geo match condition.

Hence, the correct answers are: Using AWS WAF, create a web ACL with a rule that explicitly allows requests from approved IP addresses declared in an IP Set. Add another rule in the AWS WAF web ACL with a geo match condition that blocks requests that originate from a specific country.

The option that says: In the Application Load Balancer, create a listener rule that explicitly allows requests from approved IP addresses is incorrect because a listener rule just checks for connection requests using the protocol and port that you configure. It only determines how the load balancer routes the requests to its registered targets.

The option that says: Set up a geo match condition in the Application Load Balancer that block requests that originate from a specific country is incorrect because you can't configure a geo match condition in an Application Load Balancer. You must use AWS WAF instead.

The option that says: 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 is incorrect because AWS Transit Gateway is simply a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. Using this type of gateway is not warranted in this scenario. Moreover, Network ACLs are not suitable for blocking requests from a specific country. You must use AWS WAF instead.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-geo-conditions.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html>

[Go back to Q118](#)

Answer to Q119: B

[Go back to Q119](#)

Explanation to Q119

NA

[Go back to Q119](#)

Answer to Q120: A

[Go back to Q120](#)

Explanation to Q120

Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed.

While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the EBS volume normally.

When you create an EBS volume based on a snapshot, the new volume begins as an exact replica of the original volume that was used to create the snapshot. The replicated volume loads data lazily in the background so that you can begin using it immediately. If you access data that hasn't been

loaded yet, the volume immediately downloads the requested data from Amazon S3, and then continues loading the rest of the volume's data in the background.

A non-root EBS volume can be detached or attached to a new EC2 instance while the snapshot is in progress. The only exception here is if you are taking a snapshot of your root volume.

Hence, the correct answer is: The EBS volume can be used while the snapshot is in progress.

The option that says: The EBS volume cannot be detached or attached to an EC2 instance until the snapshot completes is not entirely correct. A non-root EBS volume can be detached or attached to a new EC2 instance while the snapshot is in progress. However, you cannot do this for your root volume.

The option that says: The EBS volume can be used in read-only mode while the snapshot is in progress is incorrect because you can perform both read and write operations in the volume while the snapshot is in progress.

The option that says: The EBS volume cannot be used until the snapshot completes is incorrect because just as shown in the previous option, the volume can be used even if the snapshot process is in progress.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

[Go back to Q120](#)

Answer to Q121: C

[Go back to Q121](#)

Explanation to Q121

A "fanout" pattern is when an Amazon SNS message is sent to a topic and then replicated and pushed to multiple Amazon SQS queues, HTTP endpoints, or email addresses. This allows for parallel asynchronous processing. For example, you could develop an application that sends an Amazon SNS message to a topic whenever an order is placed for a product. Then, the Amazon SQS queues that are subscribed to that topic would receive identical notifications for the new order. The Amazon EC2 server instance attached to one of the queues could handle the processing or fulfillment of the order, while the other server instance could be attached to a data warehouse for analysis of all orders received.

When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.

Immediately after the message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The maximum is 12 hours.

The option that says: The message will automatically be assigned to the same EC2 instance when it comes back online within or after the visibility timeout is incorrect because the message will not be automatically assigned to the same EC2 instance once it is abruptly terminated. When the message visibility timeout expires, the message becomes available for processing by other EC2 instances.

The option that says: The message is deleted and becomes duplicated in the SQS when the EC2 instance comes online is incorrect because the message will not be deleted and won't be duplicated in the SQS queue when the EC2 instance comes online.

The option that says: The message will be sent to a Dead Letter Queue in AWS DataSync is incorrect because although the message could be programmatically sent to a Dead Letter Queue (DLQ), it won't be handled by AWS DataSync but by Amazon SQS instead. AWS DataSync is primarily used to simplify your migration with AWS. It makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS).

References:

<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

<https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html>

[Go back to Q121](#)

Answer to Q122: D, E

[Go back to Q122](#)

Explanation to Q122

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:- Data at rest inside the volume- All data moving between the volume and the instance- All snapshots created from the volume- All volumes created from those snapshots. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage. You can encrypt both the boot and data volumes of an EC2 instance.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

[Go back to Q122](#)

Answer to Q123: A

[Go back to Q123](#)

Explanation to Q123

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as EFS, S3 and EBS. You must understand when you should use Amazon EFS, Amazon S3 and Amazon Elastic Block Store (EBS) based on the specific workloads. In this scenario, the keywords are rapidly changing data and 1000 Linux servers.

Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the same level of high availability and high scalability like S3 however, this service is more

suitable for scenarios where it is required to have a POSIX-compatible file system or if you are storing rapidly changing data.

Data that must be updated very frequently might be better served by storage solutions that take into account read and write latencies, such as Amazon EBS volumes, Amazon RDS, Amazon DynamoDB, Amazon EFS, or relational databases running on Amazon EC2. Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.

In this scenario, EFS is the best answer. As stated above, Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the performance, durability, high availability, and storage capacity needed by the 1000 Linux servers in the scenario. S3 is incorrect because although this provides the same level of high availability and high scalability like EFS, this service is not suitable for storing data which are rapidly changing, just as mentioned in the above explanation. It is still more effective to use EFS as it offers strong consistency and file locking which the S3 service lacks.

EBS is incorrect because an EBS Volume cannot be shared by multiple instances.

Storage Gateway is incorrect because this is primarily used to extend the storage of your on-premises data center to your AWS Cloud.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

<https://aws.amazon.com/efs/features/> <https://d1.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=9>

[Go back to Q123](#)

Answer to Q124: D

[Go back to Q124](#)

Explanation to Q124

In this scenario, the application is deployed in a fleet of EC2 instances that are polling messages from a single SQS queue. Amazon SQS uses short polling by default, querying only a subset of the servers (based on a weighted random distribution) to determine whether any messages are available for inclusion in the response. Short polling works for scenarios that require higher throughput. However, you can also configure the queue to use Long polling instead, to reduce cost.

The `ReceiveMessageWaitTimeSeconds` is the queue attribute that determines whether you are using Short or Long polling. By default, its value is zero which means it is using Short polling. If it is set to a value greater than zero, then it is Long polling.

Hence, configuring Amazon SQS to use long polling by setting the `ReceiveMessageWaitTimeSeconds` to a number greater than zero is the correct answer.

Quick facts about SQS Long Polling:- Long polling helps reduce your cost of using Amazon SQS by reducing the number of empty responses when there are no messages available to return in reply to a `ReceiveMessage` request sent to an Amazon SQS queue and eliminating false empty responses when messages are available in the queue but aren't included in the response.- Long polling reduces the number of empty responses by allowing Amazon SQS to wait until a message is available in the queue before sending a response. Unless the connection times out, the response to the `ReceiveMessage` request contains at least one of the available messages, up to the maximum number of messages specified in the `ReceiveMessage` action.- Long polling eliminates false empty responses by

querying all (rather than a limited number) of the servers. Long polling returns messages as soon any message becomes available.

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-long-polling.html>

[Go back to Q124](#)

Answer to Q125: C

[Go back to Q125](#)

Explanation to Q125

NA

[Go back to Q125](#)

Answer to Q126: C

[Go back to Q126](#)

Explanation to Q126

The important concept that you must understand in the scenario is that your VPC and your S3 bucket are located within the larger AWS network. However, the traffic coming from your VPC to your S3 bucket is traversing the public Internet by default. To better protect your data in transit, you can set up a VPC endpoint so the incoming traffic from your VPC will not pass through the public Internet, but instead through the private AWS network.

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other services do not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

There are two types of VPC endpoints: interface endpoints and gateway endpoints. You should create the type of VPC endpoint required by the supported service. As a rule of thumb, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Configuring a VPC Gateway Endpoint along with a corresponding route entry that directs the data to S3 is correct because VPC Gateway Endpoint supports private connection to S3. Creating an Internet gateway in the public subnet with a corresponding route entry that directs the data to S3 is incorrect because Internet gateway is used for instances in the public subnet to have accessibility to the Internet.

Configuring a VPC Interface Endpoint along with a corresponding route entry that directs the data to S3 is incorrect because VPC Interface Endpoint does not support the S3 service. You should use a VPC Gateway Endpoint instead. As mentioned in the above explanation, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Provisioning a NAT gateway in the private subnet with a corresponding route entry that directs the data to S3 is incorrect because NAT Gateway allows instances in the private subnet to gain access to the Internet, but not vice versa.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

[Go back to Q126](#)

Answer to Q127: D

[Go back to Q127](#)

Explanation to Q127

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides you with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA). You don't have to worry about managing file servers and storage, as Amazon FSx automates the time-consuming administration tasks such as hardware provisioning, software configuration, patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.

Amazon FSx provides you with two file systems to choose from: Amazon FSx for Windows File Server for Windows-based applications and Amazon FSx for Lustre for compute-intensive workloads.

For Windows-based applications, Amazon FSx provides fully managed Windows file servers with features and performance optimized for "lift-and-shift" business-critical application workloads including home directories (user shares), media workflows, and ERP applications. It is accessible from Windows and Linux instances via the SMB protocol. If you have Linux-based applications, Amazon EFS is a cloud-native fully managed

file system that provides simple, scalable, elastic file storage accessible from Linux instances via the NFS protocol.

For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that's optimized for performance, with input and output stored on Amazon S3. Hence, the correct answer is: Amazon FSx for Windows File Server.

Amazon S3 Glacier Deep Archive is incorrect because this service is primarily used as a secure, durable, and extremely low-cost cloud storage for data archiving and long-term backup.

AWS DataSync is incorrect because this service simply provides a fast way to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). Amazon FSx for Lustre is incorrect because this service doesn't support the Windows-based applications as well as Windows servers.

References:

<https://aws.amazon.com/fsx/>
<https://aws.amazon.com/getting-started/use-cases/hpc/3/>

[Go back to Q127](#)

Answer to Q128: A

[Go back to Q128](#)

Explanation to Q128

Weighted routing lets you associate multiple resources with a single domain name (example.com) or subdomain name (acme.example.com) and choose how much traffic is routed to each resource. This can be useful

for a variety of purposes including load balancing and testing new versions of software. You can set a specific percentage of how much traffic will be allocated to the resource by specifying the weights. For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets 1/256th of the traffic ($1/1+255$), and the other resource gets 255/256ths ($255/1+255$). You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.

Reference:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

[Go back to Q128](#)

Answer to Q129: D

[Go back to Q129](#)

Explanation to Q129

NA

[Go back to Q129](#)

Answer to Q130: A

[Go back to Q130](#)

Explanation to Q130

In this scenario, the requirement is to have a storage option that is cost-effective and can access or retrieve the archived data immediately. The

cost-effective options are Amazon Glacier Deep Archive and Amazon S3 Standard- Infrequent Access (Standard - IA). However, the former option is not designed for rapid retrieval of data which is required for the surprise audit. Hence, using Amazon Glacier Deep Archive is incorrect and the best answer is to use Amazon S3 Standard - Infrequent Access.

Using Amazon S3 Standard is incorrect because the standard storage class is not cost-efficient in this scenario. It costs more than Glacier Deep Archive and S3 Standard - Infrequent Access.

Using Amazon S3 -Intelligent Tiering is incorrect because the Intelligent Tiering storage class entails an additional fee for monitoring and automation of each object in your S3 bucket vs. the Standard storage class and S3 Standard - Infrequent Access.

Amazon S3 Standard - Infrequent Access is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

This combination of low cost and high performance makes Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

References:

<https://aws.amazon.com/s3/storage-classes/>
<https://aws.amazon.com/s3/faqs/>

[Go back to Q130](#)

Answer to Q131: A

[Go back to Q131](#)

Explanation to Q131

AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances.

AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your TCP and UDP traffic. AWS Global Accelerator continually monitors the health of your application endpoints and will detect an unhealthy endpoint and redirect traffic to healthy endpoints in less than 1 minute.

Many applications, such as gaming, media, mobile applications, and financial applications, need very low latency for a great user experience. To improve the user experience, AWS Global Accelerator directs user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It routes the traffic to the closest edge location via Anycast, then by routing it to the closest regional endpoint over the AWS global network. AWS Global Accelerator quickly reacts to changes in network performance to improve your user's application performance.

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

Hence, the correct answer is AWS Global Accelerator.

Amazon CloudFront is incorrect because although this service uses edge locations, it doesn't have the capability to route the traffic to the closest edge location via an Anycast static IP address.

AWS WAF is incorrect because this service is just a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources.

AWS PrivateLink is incorrect because this service simply provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. It doesn't route traffic to the closest edge location via an Anycast static IP address.

References:

<https://aws.amazon.com/global-accelerator/>
<https://aws.amazon.com/global-accelerator/faqs/>

[Go back to Q131](#)

Answer to Q132: A

[Go back to Q132](#)

Explanation to Q132

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfer of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.

Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet. S3 Transfer Acceleration (S3TA) reduces the variability in Internet routing, congestion and speeds that can affect transfers, and logically shortens the distance to S3 for remote applications. S3TA improves transfer performance by routing traffic through Amazon CloudFront's globally distributed Edge Locations and over AWS backbone networks, and by using network protocol optimizations.

Hence, Transfer Acceleration is the correct answer.

AWS Global Accelerator is incorrect because this service is primarily used to optimize the path from your users to your applications which improves the performance of your TCP and UDP traffic. Using Amazon S3 Transfer Acceleration is a more suitable service for this scenario.

Cross-Region Replication is incorrect because this simply enables you to automatically copy S3 objects from one bucket to another bucket that is placed in a different AWS Region or within the same Region.

Multipart Upload is incorrect because this feature simply allows you to upload a single object as a set of parts. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

References:

<https://aws.amazon.com/s3/faqs/>
<https://aws.amazon.com/s3/transfer-acceleration/>

[Go back to Q132](#)

Answer to Q133: B

[Go back to Q133](#)

Explanation to Q133

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

AWS WAF is incorrect because this is a web application firewall service that helps protect your web apps from common exploits that could affect app availability, compromise security, or consume excessive resources. Although this can help you against DDoS attacks, AWS WAF alone is not enough to fully protect your VPC. You still need to use AWS Shield in this scenario.

AWS Firewall Manager is incorrect because this just simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources.

Amazon GuardDuty is incorrect because this is just an intelligent threat detection service to protect your AWS accounts and workloads. Using this alone will not fully protect your AWS resources against DDoS attacks.

References:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-which-to-choose.html>

<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

[Go back to Q133](#)

Answer to Q134: C

[Go back to Q134](#)

Explanation to Q134

NA

[Go back to Q134](#)

Answer to Q135: A

[Go back to Q135](#)

Explanation to Q135

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple

copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, Oracle and PostgreSQL as well as Amazon Aurora.

Enabling Multi-AZ deployments is incorrect because the Multi-AZ deployments feature is mainly used to achieve high availability and failover support for your database.

Enabling Amazon RDS Standby Replicas is incorrect because a Standby replica is used in Multi-AZ deployments and hence, it is not a solution to reduce read-heavy database workloads.

Using SQS to queue up the requests is incorrect because although an SQS queue can effectively manage the requests, it won't be able to entirely improve the read-throughput of the database by itself.

References:

<https://aws.amazon.com/rds/details/read-replicas/>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadReplica.html

[Go back to Q135](#)

Answer to Q136: D

[Go back to Q136](#)

Explanation to Q136

Two important requirements that the chosen AWS service should fulfill is that data should not go missing, is durable, and streams data in the sequence of arrival. Kinesis can do the job just fine because of its

architecture. A Kinesis data stream is a set of shards that has a sequence of data records, and each data record has a sequence number that is assigned by Kinesis Data Streams. Kinesis can also easily handle the high volume of messages being sent to the service.

Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering). Setting up a default Amazon SQS queue to handle the messages is incorrect because although SQS is a valid messaging service, it is not suitable for scenarios where you need to process the data based on the order they were received. Take note that a default queue in SQS is just a standard queue and not a FIFO (First-In-First-Out) queue. In addition, SQS does not guarantee that no duplicates will be sent.

Setting up an Amazon SNS Topic to handle the messages is incorrect because SNS is a pub-sub messaging service in AWS. SNS might not be capable of handling such a large volume of messages being received and sent at a time. It does not also guarantee that the data will be transmitted in the same order they were received.

Creating a pipeline using AWS Data Pipeline to handle the messages is incorrect because this is primarily used as a cloud-based data workflow service that helps you process and move data between different AWS services and on-premises data sources. It is not suitable for collecting data from distributed sources such as users, IoT devices, or clickstreams.

References:

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

For additional information, read the When should I use Amazon Kinesis Data Streams, and when should I use Amazon SQS? section of the Kinesis

Data Stream FAQ:

<https://aws.amazon.com/kinesis/data-streams/faqs/>

[Go back to Q136](#)

Answer to Q137: D

[Go back to Q137](#)

Explanation to Q137

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.

Today, you can connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time-consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With AWS Transit Gateway, you only must create and manage a single connection from the central gateway to each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes.

This hub and spoke model significantly simplify management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other

network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.

It acts as a Regional virtual router for traffic flowing between your virtual private clouds (VPC) and VPN connections. A transit gateway scales elastically based on the volume of network traffic. Routing through a transit gateway operates at layer 3, where the packets are sent to a specific next-hop attachment, based on their destination IP addresses.

A transit gateway attachment is both a source and a destination of packets. You can attach the following resources to your transit gateway:- One or more VPCs- One or more VPN connections- One or more AWS Direct Connect gateways- One or more transit gateway peering connections.

If you attach a transit gateway peering connection, the transit gateway must be in a different Region.

Hence, the correct answer is: Set up an AWS Transit Gateway to implement a hub-and-spoke network topology in each region that routes all traffic through a network transit center. Route traffic between VPCs and the on-premises data centers over AWS Site-to-Site VPNs.

The option that says: Set up an AWS Direct Connect Gateway to achieve inter-region VPC access to all the AWS resources and on-premises 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 is incorrect because you can only create a private virtual interface to a Direct Connect gateway and not a public virtual interface.

Using a link aggregation group (LAG) is also irrelevant in this scenario because it is just a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

The option that says: Enable inter-region VPC peering which allows peering relationships to be established between VPCs across different AWS regions. This will ensure that the traffic will always stay on the global AWS backbone and will never traverse the public Internet is incorrect because this solution would require a lot of manual setup and management overhead to successfully build a functional, error-free inter-region VPC network compared with just using a Transit Gateway. Although the Inter-Region VPC Peering provides a cost-effective way to share resources between regions or replicate data for geographic redundancy, its connections are not dedicated and highly available. Moreover, it doesn't support the company's on-premises data centers in multiple AWS Regions.

The option that says: 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 is incorrect because this solution doesn't meet the requirement of interconnecting all of the company's on-premises networks, VPNs, and VPCs into a single gateway, that includes support for inter-region peering across multiple AWS regions. As its name implies, the AWS VPN CloudHub is only for VPNs and not for VPCs. It is also not capable of managing hundreds of VPCs with multiple VPN connections to their data centers that span to multiple AWS Regions.

References:

<https://aws.amazon.com/transit-gateway/>

<https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html>

[Go back to Q137](#)

Answer to Q138: B

[Go back to Q138](#)

Explanation to Q138

You can create a lifecycle policy in S3 to automatically transfer your data to Glacier.

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects.

These actions can be classified as follows:

Transition actions : In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.

Expiration actions: In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

[Go back to Q138](#)

Answer to Q139: A, E

[Go back to Q139](#)

Explanation to Q139

NA

[Go back to Q139](#)

Answer to Q140: A

[Go back to Q140](#)

Explanation to Q140

NA

[Go back to Q140](#)

Answer to Q141: C

[Go back to Q141](#)

Explanation to Q141

You can run an Amazon RDS DB instance in several AZs with Multi-AZ deployment. Amazon automatically provisions and maintains a secondary standby DB instance in a different AZ. Your primary DB instance is synchronously replicated across AZs to the secondary instance to provide data redundancy, failover support, eliminate I/O freezes, and minimize latency spikes during systems backup.

As described in the scenario, the architecture must meet two requirements:

1. The database should automatically failover to an RDS instance in case of failures.
2. The architecture should be as highly available as possible.

Hence, the correct answer is: Create a standby replica in another availability zone by enabling Multi-AZ deployment because it meets both requirements.

The option that says: 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 is incorrect. Although this architecture provides higher availability since it can survive a region failure, it still does not meet the first requirement since the process is not automated. The architecture should also support automatic failover to an RDS instance in case of failures.

Both the following options are incorrect:- Create five read replicas across different availability zones. In the event of an Availability Zone outage, promote any replica to become the primary instance- 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.

Although it is possible to achieve high availability with these architectures by promoting a read replica into the primary instance in an event of failure, it does not support automatic failover to an RDS instance which is also a requirement in the problem.

References:

<https://aws.amazon.com/rds/features/multi-az/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

[Go back to Q141](#)

Answer to Q142: A

[Go back to Q142](#)

Explanation to Q142

You can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for an Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration.

Hence, the correct answer is: Create a new launch configuration with the new instance type and update the Auto Scaling Group.

The option that says: Just change the instance type to t2.2xlarge in the current launch configuration is incorrect because you can't change your launch configuration once it is created. You must create a new one instead.

The option that says: Create another Auto Scaling Group and attach the new instance type is incorrect because you can't directly attach or declare the new instance type to your Auto Scaling group. You must create a new launch configuration first, with a new instance type, then attach it to your existing Auto Scaling group.

The option that says: Change the instance type of each EC2 instance manually is incorrect because you can't directly change the instance type of your EC2 instance. This should be done by creating a brand-new launch configuration then attaching it to your existing Auto Scaling group.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg.html>

[Go back to Q142](#)

Answer to Q143: A

[Go back to Q143](#)

Explanation to Q143

An Amazon S3 Glacier (Glacier) vault can have one resource-based vault access policy and one Vault Lock policy attached to it. A Vault Lock policy is a vault access policy that you can lock. Using a Vault Lock policy can help you enforce regulatory and compliance requirements. Amazon S3 Glacier provides a set of API operations for you to manage the Vault Lock policies.

As an example of a Vault Lock policy, suppose that you are required to retain archives for one year before you can delete them. To implement this requirement, you can create a Vault Lock policy that denies users permissions to delete an archive until the archive has existed for one year. You can test this policy before locking it down. After you lock the policy, the policy becomes immutable. For more information about the locking process, see Amazon S3 Glacier Vault Lock. If you want to manage other user permissions that can be changed, you can use the vault access policy.

Amazon S3 Glacier supports the following archive operations: Upload, Download, and Delete. Archives are immutable and cannot be modified. Hence, the correct answer is to store the audit logs in a Glacier vault and use the Vault Lock feature.

Storing the audit logs in an EBS volume and then taking EBS snapshots every month is incorrect because this is not a suitable and secure solution. Anyone who has access to the EBS Volume can simply delete and modify the audit logs. Snapshots can be deleted too.

Storing the audit logs in an Amazon S3 bucket and enabling Multi-Factor Authentication Delete (MFA Delete) on the S3 bucket is incorrect because this would still not meet the requirement. If someone has access to the S3 bucket and has the proper MFA privileges, then the audit logs can be edited.

Storing the audit logs in an EFS volume and using Network File System version 4 (NFSv4) file-locking mechanism is incorrect because the data integrity of the audit logs can still be compromised if it is stored in an EFS volume with Network File System version 4 (NFSv4) file-locking mechanism and hence, not suitable as storage for the files. Although it will provide some sort of security, the file lock can still be overridden, and the audit logs might be edited by someone else.

References:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

<https://aws.amazon.com/blogs/aws/glacier-vault-lock/>

[Go back to Q143](#)

Answer to Q144: C

[Go back to Q144](#)

Explanation to Q144

NA

[Go back to Q144](#)

Answer to Q145: B

[Go back to Q145](#)

Explanation to Q145

The main differences are that:- Spot instances typically offer a significant discount off the On-Demand prices.- Your instances can be interrupted by Amazon EC2 for capacity requirements with a 2-minute notification.- Spot prices adjust gradually based on long term supply and demand for spare EC2 capacity.

You can choose to have your Spot instances terminated, stopped, or hibernated upon interruption. Stop and hibernate options are available for persistent Spot requests and Spot Fleets with the maintain option enabled.

By default, your instances are terminated hence, the correct answer is the option that says: The instance will be terminated.

Reference:

<https://aws.amazon.com/ec2/faqs/>

[Go back to Q145](#)

Answer to Q146: D

[Go back to Q146](#)

Explanation to Q146

You can use AWS X-Ray to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available.

X-Ray gives you an end-to-end view of an entire request, so you can analyze latencies in your APIs and their backend services. You can use an X-Ray service map to view the latency of an entire request and that of the downstream services that are integrated with X-Ray. And you can configure

sampling rules to tell X-Ray which requests to record, at what sampling rates, according to criteria that you specify. If you call an API Gateway API from a service that's already being traced, API Gateway passes the trace through, even if X-Ray tracing is not enabled on the API.

You can enable X-Ray for an API stage by using the API Gateway management console, or by using the API Gateway API or CLI. VPC Flow Logs is incorrect because this is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your entire VPC. Although it can capture some details about the incoming user requests, it is still better to use AWS X-Ray as it provides a better way to debug and analyze your microservices applications with request tracing so you can find the root cause of your issues and performance.

CloudWatch is incorrect because this is a monitoring and management service. It does not have the capability to trace and analyze user requests as they travel through your Amazon API Gateway APIs.

CloudTrail is incorrect because this is primarily used for IT audits and API logging of all your AWS resources. It does not have the capability to trace and analyze user requests as they travel through your Amazon API Gateway APIs, unlike AWS X-Ray.

Reference:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-xray.html>

[Go back to Q146](#)

Answer to Q147: D

[Go back to Q147](#)

[Explanation to Q147](#)

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.

An io1 volume can range in size from 4 GiB to 16 TiB. You can provision from 100 IOPS up to 64,000 IOPS per volume on Nitro system instance families and up to 32,000 on other instance families. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. On a supported instance type, any volume 1,280 GiB in size or greater allows provisioning up to the 64,000 IOPS maximum ($50 \times 1,280 \text{ GiB} = 64,000$). An io1 volume provisioned with up to 32,000 IOPS supports a maximum I/O size of 256 KiB and yields as much as 500 MiB/s of throughput. With the I/O size at the maximum, peak throughput is reached at 2,000 IOPS. A volume provisioned with more than 32,000 IOPS (up to the cap of 64,000 IOPS) supports a maximum I/O size of 16 KiB and yields as much as 1,000 MiB/s of throughput.

The volume queue length is the number of pending I/O requests for a device. Latency is the true end-to-end client time of an I/O operation, in other words, the time elapsed between sending an I/O to EBS and receiving an acknowledgement from EBS that the I/O read or write is complete. Queue length must be correctly calibrated with I/O size and latency to avoid creating bottlenecks either on the guest operating system or on the network link to EBS.

Optimal queue length varies for each workload, depending on your application's sensitivity to IOPS and latency. If your workload is not delivering enough I/O requests to fully use the performance available to your EBS volume, then your volume might not deliver the IOPS or throughput that you have provisioned.

Transaction-intensive applications are sensitive to increased I/O latency and are well-suited for SSD-backed io1 and gp2 volumes. You can maintain high IOPS while keeping latency down by maintaining a low queue length and a high number of IOPS available to the volume. Consistently driving more IOPS to a volume than it has available can cause increased I/O latency.

Throughput-intensive applications are less sensitive to increased I/O latency and are well-suited for HDD-backed st1 and sc1 volumes. You can maintain high throughput to HDD-backed volumes by maintaining a high queue length when performing large, sequential I/O.

Therefore, for instance, a 10 GiB volume can be provisioned with up to 500 IOPS. Any volume 640 GiB in size or greater allows provisioning up to a maximum of 32,000 IOPS ($50 \text{ GiB} / 640 \text{ GiB} = 32,000$). Hence, the correct answer is to set the IOPS to 500 then maintain a low queue length.

Setting the IOPS to 400 then maintaining a low queue length is incorrect because although a value of 400 is an acceptable value, it is not the maximum value for the IOPS. You will not fully utilize the available IOPS that the volume can offer if you just set it to 400. The options that say: Set the IOPS to 600 then maintain a high queue length and Set the IOPS to 800 then maintain a low queue length are both incorrect because the maximum IOPS for the 10 GiB volume is only 500. Therefore, any value greater than the maximum amount, such as 600 or 800, is wrong. Moreover, you should keep the latency down by maintaining a low queue length, and not higher.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html>

[Go back to Q147](#)

Answer to Q148: A, C

[Go back to Q148](#)

Explanation to Q148

The global news website has a problem with latency considering that there are a lot of readers of the site from all parts of the globe. In this scenario, you can use a content delivery network (CDN) which is a geographically distributed group of servers which work together to provide fast delivery of Internet content. And since this is a news website, most of its data are read-only, which can be cached to improve the read throughput and avoid the repetitive requests from the server.

In AWS, Amazon CloudFront is the global content delivery network (CDN) service that you can use and for web caching, Amazon ElastiCache is the suitable service. Hence, the correct answers here are using Amazon CloudFront with website as the custom origin and using Amazon ElastiCache for the website's in-memory data store or cache.

The option that says: For better read throughput, use AWS Storage Gateway to distribute the content across multiple regions is incorrect as AWS Storage Gateway is used for storage.

Deploying the website to all regions in different VPCs for faster processing is incorrect as this would be costly and totally unnecessary considering that you can use Amazon CloudFront and ElastiCache to improve the performance of the website.

References:

<https://aws.amazon.com/elasticsearch/http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

[Go back to Q148](#)

Answer to Q149: A

[Go back to Q149](#)

Explanation to Q149

AWS Step Functions provides serverless orchestration for modern applications. Orchestration centrally manages a workflow by breaking it into multiple steps, adding flow logic, and tracking the inputs and outputs between the steps. As your applications execute, Step Functions maintains application state, tracking exactly which workflow step your application is in, and stores an event log of data that is passed between application components. That means that if networks fail or components hang, your application can pick up right where it left off.

Application development is faster and more intuitive with Step Functions, because you can define and manage the workflow of your application independently from its business logic. Making changes to one does not affect the other. You can easily update and modify workflows in one place, without having to struggle with managing, monitoring and maintaining multiple point-to-point integrations. Step Functions frees your functions and containers from excess code, so your applications are faster to write, more resilient, and easier to maintain. SWF is incorrect because this is a fully-managed state tracker and task coordinator service. It does not provide serverless orchestration to multiple AWS resources.

AWS Lambda is incorrect because although Lambda is used for serverless computing, it does not provide a direct way to coordinate multiple AWS services into serverless workflows.

AWS Batch is incorrect because this is primarily used to efficiently run hundreds of thousands of batch computing jobs in AWS.

Reference:

<https://aws.amazon.com/step-functions/features/>

[Go back to Q149](#)

Answer to Q150: C

[Go back to Q150](#)

Explanation to Q150

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of having to wait until all your data is collected before the processing can begin.

Redshift Spectrum is incorrect because this is primarily used to directly query open data formats stored in Amazon S3 without the need for unnecessary data movement, which enables you to analyze data across your data warehouse and data lake, together, with a single service. It does not provide the ability to process your data in real-time, unlike Kinesis.

AWS Glue is incorrect because this is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It does not provide the ability to process your data in real-time, unlike Kinesis.

Amazon EMR with Compute Optimized Instances is incorrect because this is a web service that uses an open-source Hadoop framework to quickly & cost-effectively process vast amounts of data. It does not provide the ability to process your data in real-time, unlike Kinesis. Compute-optimized instances are ideal for compute-bound applications that benefit from high-

performance processors but not for analyzing clickstream data from various websites in real-time.

References:

<https://aws.amazon.com/kinesis/https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html>

[Go back to Q150](#)

Answer to Q151: B, C

[Go back to Q151](#)

Explanation to Q151

If you got your certificate from a third-party CA, import the certificate into ACM or upload it to the IAM certificate store. Hence, AWS Certificate Manager and IAM certificate store are the correct answers.

ACM lets you import third-party certificates from the ACM console, as well as programmatically. If ACM is not available in your region, use AWS CLI to upload your third-party certificate to the IAM certificate store.

A private S3 bucket with versioning enabled and an S3 bucket configured with server-side encryption with customer-provided encryption keys (SSE-C) are both incorrect as S3 is not a suitable service to store the SSL certificate.

CloudFront is incorrect because although you can upload certificates to CloudFront, it doesn't mean that you can import SSL certificates on it. You would not be able to export the certificate that you have loaded in CloudFront nor assign them to your EC2 or ELB instances as it would be tied to a single CloudFront distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html#cnames-and-https-uploading-certificates>

[Go back to Q151](#)

Answer to Q152: A, E

[Go back to Q152](#)

Explanation to Q152

Server-side encryption is the encryption of data at its destination by the application or service that receives it. AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud.

Amazon S3 uses AWS KMS customer master keys (CMKs) to encrypt your Amazon S3 objects. SSE-KMS encrypts only the object data. Any object metadata is not encrypted. If you use customer-managed CMKs, you use AWS KMS via the AWS Management Console or AWS KMS APIs to centrally create encryption keys, define the policies that control how keys can be used, and audit key usage to prove that they are being used correctly. You can use these keys to protect your data in Amazon S3 buckets.

A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. You can use a CMK to encrypt and decrypt up to 4 KB (4096 bytes) of data. Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of AWS KMS to encrypt your data. This strategy is known as envelope encryption.

You have three mutually exclusive options depending on how you choose to manage the encryption keys:

1. Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) Each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.
2. Use Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) Similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer-managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region.
3. Use Server-Side Encryption with Customer-Provided Keys (SSE-C) You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption when you access your objects.

In the scenario, the company needs to store financial files in AWS which are accessed every week and the solution should use envelope encryption. This requirement can be fulfilled by using an Amazon S3 configured with Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS). Hence, using Amazon S3 to store the data and configuring Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) are the correct answers.

Using Amazon S3 Glacier Deep Archive to store the data is incorrect because although this provides the most cost-effective storage solution, it

is not the appropriate service to use if the files being stored are frequently accessed every week.

Configuring Server-Side Encryption with Customer-Provided Keys (SSE-C) and configuring Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) are incorrect because although you can configure automatic key rotation, these two do not provide you with an audit trail that shows when your CMK was used and by whom, unlike Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html>

[Go back to Q152](#)

Answer to Q153: C

[Go back to Q153](#)

Explanation to Q153

Initially, the files will be accessed frequently, and S3 is a durable and highly available storage solution for that. After a month has passed, the files won't be accessed frequently anymore, so it is a good idea to use lifecycle policies to move them to a storage class that would have a lower cost for storing them.

Since the files are easily reproducible and some of them are needed to be retrieved quickly based on a specific prefix filter (techradio-finance), S3-One Zone IA would be a good choice for storing them. The other files that do not contain such prefix would then be moved to Glacier for low cost archival. This setup would also be the most cost-effective for the client.

Hence, the correct answer is to store the files in S3 then after a month, change the storage class of the techradio-finance prefix to One Zone-IA while the remaining go to Glacier using lifecycle policy.

Storing the files in S3 then after a month, changing the storage class of the bucket to S3-IA using lifecycle policy is incorrect because although it is valid to move the files to S3-IA, this solution still costs more compared with using a combination of S3-One Zone IA and Glacier.

Storing the files in S3 then after a month, changing the storage class of the bucket to Intelligent-Tiering using lifecycle policy is incorrect because while S3 Intelligent-Tiering can automatically move data between two access tiers (frequent access and infrequent access) when access patterns change, it is more suitable for scenarios where you don't know the access patterns of your data. It may take some time for S3 Intelligent-Tiering to analyze the access patterns before it moves the data to a cheaper storage class like S3-IA which means you may still end up paying more in the beginning. In addition, you already know the access patterns of the files which means you can directly change the storage class immediately and save cost right away.

Storing the files in S3 then after a month, changing the storage class of the techradio-finance prefix to S3-IA while the remaining go to Glacier using lifecycle policy is incorrect because although S3-IA costs less than S3 Standard storage class, it is still more expensive than S3-One Zone IA. Remember that the files are easily reproducible so you can safely move the data to S3-One Zone IA and in case there is an outage, you can simply generate the missing data again.

References:

<https://aws.amazon.com/blogs/compute/amazon-s3-adds-prefix-and-suffix-filters-for-lambda-function-triggering>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-configuration-examples.html>

<https://aws.amazon.com/s3/pricing>

[Go back to Q153](#)

Answer to Q154: A

[Go back to Q154](#)

Explanation to Q154

When you launch an EC2 instance into a default VPC, AWS provides it with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

However, when you launch an instance into a non-default VPC, AWS provides the instance with a private DNS hostname only. New instances will only be provided with public DNS hostname depending on these two DNS attributes: the DNS resolution and DNS hostnames, that you have specified for your VPC, and if your instance has a public IPv4 address.

In this case, the new EC2 instance does not automatically get a DNS hostname because the DNS resolution and DNS hostnames attributes are disabled in the newly created VPC.

The option that says: The newly created VPC has an invalid CIDR block is incorrect since it's very unlikely that a VPC has an invalid CIDR block

because of AWS validation schemes.

The option that says: Amazon Route 53 is not enabled is incorrect since Route 53 does not need to be enabled. Route 53 is the DNS service of AWS, but the VPC is the one that enables assigning of instance hostnames.

The option that says: The security group of the EC2 instance needs to be modified is incorrect since security groups are just firewalls for your instances. They filter traffic based on a set of security group rules.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html>

<https://aws.amazon.com/vpc/>

[Go back to Q154](#)

Answer to Q155: C

[Go back to Q155](#)

Explanation to Q155

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms.

Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

AWS CloudTrail is incorrect as this is mainly used for logging and not for monitoring.

Amazon SWF and Amazon SQS are incorrect as both are used for creating distributed application with decoupled components and not for monitoring.

Reference:

<https://aws.amazon.com/cloudwatch/faqs/>

[Go back to Q155](#)

Answer to Q156: D

[Go back to Q156](#)

Explanation to Q156

An Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications. EFA enables you to achieve the application performance of an on-premises HPC cluster, with the scalability, flexibility, and elasticity provided by the AWS Cloud.

EFA provides lower and more consistent latency and higher throughput than the TCP transport traditionally used in cloud-based HPC systems. It enhances the performance of inter-instance communication that is critical for scaling HPC and machine learning applications. It is optimized to work on the existing AWS network infrastructure, and it can scale depending on application requirements.

EFA integrates with Libfabric 1.9.0 and it supports Open MPI 4.0.2 and Intel MPI 2019 Update 6 for HPC applications, and Nvidia Collective Communications Library (NCCL) for machine learning applications.

The OS-bypass capabilities of EFAs are not supported on Windows instances. If you attach an EFA to a Windows instance, the instance functions as an Elastic Network Adapter, without the added EFA capabilities.

Elastic Network Adapters (ENAs) provide traditional IP networking features that are required to support VPC networking. EFAs provide all the same traditional IP networking features as ENAs, and they also support OS-bypass capabilities. OS-bypass enables HPC and machine learning applications to bypass the operating system kernel and to communicate directly with the EFA device.

Hence, the correct answer is to attach an Elastic Fabric Adapter (EFA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC). Attaching an Elastic Network Adapter (ENA) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because Elastic Network Adapter (ENA) doesn't have OS-bypass capabilities, unlike EFA.

Attaching an Elastic Network Interface (ENI) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because an Elastic Network Interface (ENI) is simply a logical networking component in a VPC that represents a virtual network card. It doesn't have OS-bypass capabilities that allow the HPC to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality.

Attaching a Private Virtual Interface (VIF) on each Amazon EC2 instance to accelerate High Performance Computing (HPC) is incorrect because Private Virtual Interface just allows you to connect to your VPC resources on your private IP address or endpoint.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena>

[Go back to Q156](#)

Answer to Q157: C

[Go back to Q157](#)

Explanation to Q157

NA

[Go back to Q157](#)

Answer to Q158: D

[Go back to Q158](#)

Explanation to Q158

To ensure that a Classic Load Balancer stops sending requests to instances that are de-registering or unhealthy while keeping the existing connections open, use connection draining. This enables the load balancer to complete in-flight requests made to instances that are de-registering or unhealthy. Hence, configuring Connection Draining is the correct answer.

When you enable connection draining, you can specify a maximum time for the load balancer to keep connections alive before reporting the instance as de-registered. The maximum timeout value can be set between 1 and 3,600 seconds (the default is 300 seconds). When the maximum time limit is reached, the load balancer forcibly closes connections to the de-registering instance.

Configuring Sticky Sessions is incorrect because the sticky sessions feature is mainly used to ensure that all requests from the user during the session are sent to the same instance.

Configuring both Cross-Zone Load Balancing and Sticky Sessions is incorrect because this will still not satisfy the requirement. Cross-Zone load balancing is mainly used to distribute requests evenly across the registered instances in all enabled Availability Zones. You have to enable Connection Draining.

Configuring Proxy Protocol is incorrect because this is an Internet protocol used to carry connection information from the source requesting the connection to the destination for which the connection was requested.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html>

[Go back to Q158](#)

Answer to Q159: B, E

[Go back to Q159](#)

Explanation to Q159

Amazon SQS FIFO (First-In-First-Out) Queues have all the capabilities of the standard queue with additional capabilities designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated, for example:- Ensure that user-entered commands are executed in the right order. - Display the correct product price by sending price modifications in the right order.- Prevent a student from enrolling in a course before registering for an account.

Amazon SWF provides useful guarantees around task assignments. It ensures that a task is never duplicated and is assigned only once. Thus, even though you may have multiple workers for an activity type (or a

number of instances of a decider), Amazon SWF will give a specific task to only one worker (or one decider instance). Additionally, Amazon SWF keeps at most one decision task outstanding at a time for a workflow execution. Thus, you can run multiple decider instances without worrying about two instances operating on the same execution simultaneously. These facilities enable you to coordinate your workflow without worrying about duplicate, lost, or conflicting tasks.

The main issue in this scenario is that the order management system produces duplicate orders at times. Since the company is using SQS, there is a possibility that a message can have a duplicate in case an EC2 instance failed to delete the already processed message. To prevent this issue from happening, you must use Amazon Simple Workflow service instead of SQS.

Therefore, the correct answers are:- Replace Amazon SQS and instead, use Amazon Simple Workflow service.- Use an Amazon SQS FIFO Queue instead.

Altering the retention period in Amazon SQS is incorrect because the retention period simply specifies if the Amazon SQS should delete the messages that have been in a queue for a certain period.

Altering the visibility timeout of SQS is incorrect because for standard queues, the visibility timeout isn't a guarantee against receiving a message twice. To avoid duplicate SQS messages, it is better to design your applications to be idempotent (they should not be affected adversely when processing the same message more than once). Changing the message size in SQS is incorrect because this is not related at all in this scenario.

References:

<https://aws.amazon.com/swf/faqs/>

<https://aws.amazon.com/swf/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

[Go back to Q159](#)

Answer to Q160: A, E

[Go back to Q160](#)

Explanation to Q160

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice.

CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

In RDS, the Enhanced Monitoring metrics shown in the Process List view are organized as follows:

1. RDS child processes Shows a summary of the RDS processes that support the DB instance, for example aurora for Amazon Aurora DB clusters and mysqld for MySQL DB instances.
2. Process threads appear nested beneath the parent process. Process threads show CPU utilization only as other metrics are the same for all threads for the process. The console displays a maximum of 100 processes and threads. The results are a combination of the top CPU consuming and memory consuming processes and threads. If there are more than 50

processes and more than 50 threads, the console displays the top 50 consumers in each category. This display helps you identify which processes are having the greatest impact on performance.

3. RDS processes Shows a summary of the resources used by the RDS management agent, diagnostics monitoring processes, and other AWS processes that are required to support RDS DB instances.

4. OS processes Shows a summary of the kernel and system processes, which generally have minimal impact on performance.

CPU Utilization, Database Connections, and Freeable Memory are incorrect because these are just the regular items provided by Amazon RDS Metrics in CloudWatch. Remember that the scenario is asking for the Enhanced Monitoring metrics.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html>

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs

[Go back to Q160](#)

Answer to Q161: A

[Go back to Q161](#)

Explanation to Q161

NA

[Go back to Q161](#)

Answer to Q162: D

[Go back to Q162](#)

Explanation to Q162

You can configure Amazon Redshift to copy snapshots for a cluster to another region. To configure cross-region snapshot copy, you need to enable this copy feature for each cluster and configure where to copy snapshots and how long to keep copied automated snapshots in the destination region. When cross-region copy is enabled for a cluster, all new manual and automatic snapshots are copied to the specified region.

The option that says: 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 is incorrect because although this option is possible, this entails a lot of manual work and hence, not the best option. You should configure cross-region snapshot copy instead.

The option that says: Do nothing because Amazon Redshift is a highly available, fully-managed data warehouse which can withstand an outage of an entire AWS region is incorrect because although Amazon Redshift is a fully-managed data warehouse, you will still need to configure cross-region snapshot copy to ensure that your data is properly replicated to another region.

Using Automated snapshots of your Redshift Cluster is incorrect because using automated snapshots is not enough and will not be available in case the entire AWS region is down.

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>

[Go back to Q162](#)

Answer to Q163: B

[Go back to Q163](#)

Explanation to Q163

The given scenario indicated 4 requirements that should be met in order to successfully migrate their two-tier environment from their on-premises data center to AWS Cloud. The first requirement means that you must use an application load balancer (ALB) to distribute the incoming traffic to your application servers.

The second requirement specifies that both your application and database tier should not be accessible from the public Internet. This means that you could create a single private subnet for both of your application and database tier. However, the third requirement mentioned that the database tier should not share the same subnet with other AWS resources to protect its sensitive data. This means that you should provision one private subnet for your application tier and another private subnet for your database tier.

The last requirement alludes to the need for using at least two Availability Zones to achieve high availability. This means that you must distribute your application servers to two AZs as well as your database which can be set up with a master-slave configuration to properly replicate the data between two zones.

If you have more than one private subnet in the same Availability Zone that contains instances that need to be registered with the load balancer, you only need to create one public subnet. You need only one public subnet

per Availability Zone; you can add the private instances in all the private subnets that reside in that Availability Zone.

Since you have a public internet-facing load balancer that has a group of backend Amazon EC2 instances that are deployed in a private subnet, you must create the corresponding public subnets in the same Availability Zones. This new public subnet is on top of the private subnet that is used by your private EC2 instances. Lastly, you should associate these public subnets to the internet-facing load balancer to complete the setup.

To summarize, we need to have one private subnet for the application tier and another one for the database tier. We then need to create another public subnet in the same Availability Zone where the private EC2 instances are hosted, in order to properly connect the public Internet-facing load balancer to your instances. This means that we must use a total of 3 subnets consisting of 2 private subnets and 1 public subnet.

To meet the requirement of high availability, we must deploy the stack to two Availability Zones. This means that you must double the number of subnets you are using. Take note as well that you must create the corresponding public subnet in the same Availability Zone of your private EC2 servers for it to properly communicate with the load balancer.

Hence, the correct answer is 6 subnets.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

[Go back to Q163](#)

Answer to Q164: C

[Go back to Q164](#)

Explanation to Q164

In this scenario, you can use Amazon S3 and Amazon S3 Glacier as a storage service. And since we are looking for the best option, we must consider that the object data being stored by the bank is used daily as well. Hence, Amazon S3 is the better choice as it provides frequent access to your object data.

Amazon S3 is a durable, secure, simple, and fast storage service designed to make web-scale computing easier for developers. Use Amazon S3 if you need low latency or frequent access to your data. Use Amazon S3 Glacier if low storage cost is paramount, and you do not require millisecond access to your data.

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html>

[Go back to Q164](#)

Answer to Q165: A

[Go back to Q165](#)

Explanation to Q165

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read

replicas are available in Amazon RDS for MySQL, MariaDB, Oracle and PostgreSQL, as well as Amazon Aurora.

You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. These replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

Because read replicas can be promoted to master status, they are useful as part of a sharding implementation. To shard your database, add a read replica and promote it to master status, then, from each of the resulting DB Instances, delete the data that belongs to the other shard.

Hence, the correct answer is: 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.

The option that says: 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 is incorrect because Redshift is primarily used for OLAP (Online Analytical Processing) applications and not for OLTP.

The option that says: 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 is incorrect because you can't directly connect to the standby instance. This is only used in the event of a database failover when your primary instance encountered an outage.

The option that says: Upgrade the instance type of the RDS database to a large instance is incorrect because this entails a significant amount of cost. Moreover, the production database could still be affected by the queries done by the Data Analytics team. A better solution for this scenario is to use a Read Replica instead.

References:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/rds/details/read-relicas/>

<https://aws.amazon.com/elasticache/>

[Go back to Q165](#)

Answer to Q166: A

[Go back to Q166](#)

Explanation to Q166

To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers both a new unified CloudWatch agent, and an older CloudWatch Logs agent.

It is recommended to use the unified CloudWatch agent which has the following advantages:

- You can collect both logs and advanced metrics with the installation and configuration of just one agent
- The unified agent enables the collection of logs from servers running Windows Server
- If you are using the agent to collect CloudWatch metrics, the unified agent also enables the collection of additional system metrics, for in-guest visibility
- The unified agent provides better performance

CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you quickly and effectively respond to operational issues. If an issue occurs,

you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

CloudWatch Logs Insights includes a purpose-built query language with a few simple but powerful commands. CloudWatch Logs Insights provides sample queries, command descriptions, query autocomplete, and log field discovery to help you get started quickly. Sample queries are included for several types of AWS service logs.

The option that says: 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 is incorrect.

Although this is a valid solution, this entails a lot of effort to implement as you must allocate time to install the AWS SDK to each instance and develop a custom monitoring solution. Remember that the question is specifically looking for a solution that can be implemented with minimal effort. In addition, it is unnecessary and not cost-efficient to enable detailed monitoring in CloudWatch in order to meet the requirements of this scenario since this can be done using CloudWatch Logs.

The option that says: 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 is incorrect as although this is also a valid solution, it is more efficient to use CloudWatch agent than an SSM agent. Manually connecting to an instance to view log files and troubleshoot an issue with SSM Agent is time-consuming hence, for more efficient instance monitoring, you can use the CloudWatch Agent instead to send the log data to Amazon CloudWatch Logs.

The option that says: 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 is incorrect because AWS Inspector is simply a security assessments service

which only helps you in checking for unintended network accessibility of your EC2 instances and for vulnerabilities on those EC2 instances.

Furthermore, setting up an Amazon CloudWatch dashboard is not suitable since its primarily used for scenarios where you must monitor your resources in a single view, even those resources that are spread across different AWS Regions. It is better to use CloudWatch Logs Insights instead since it enables you to interactively search and analyze your log data.

References:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

<https://docs.aws.amazon.com/systems-manager/latest/userguide/monitoring-ssm-agent.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AnalyzingLogData.html>

[Go back to Q166](#)

Answer to Q167: B

[Go back to Q167](#)

Explanation to Q167

CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view events in the CloudTrail console by going to Event history.

Event history allows you to view, search, and download the past 90 days of supported activity in your AWS account. In addition, you can create a

CloudTrail trail to further archive, analyze, and respond to changes in your AWS resources. A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify.

You can also deliver and analyze events in a trail with Amazon CloudWatch Logs and Amazon CloudWatch Events. You can create a trail with the CloudTrail console, the AWS CLI, or the CloudTrail API.

The rest of the answers are incorrect. DynamoDB and an RDS instance are for database; Amazon Redshift is used for data warehouse that scales horizontally and allows you to store terabytes and petabytes of data.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

<https://aws.amazon.com/cloudtrail/>

[Go back to Q167](#)

Answer to Q168: D

[Go back to Q168](#)

Explanation to Q168

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as Amazon S3, EFS and EBS. Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.

Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere. Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can

deliver performance for workloads that require the lowest-latency access to data from a single EC2 instance. You can also increase EBS storage for up to 16TB or add new volumes for additional storage.

In this scenario, the company is looking for a storage service which can provide the lowest-latency access to their data which will be fetched by a single m5ad.24xlarge Reserved EC2 instance. This type of workloads can be supported better by using either EFS or EBS but in this case, the latter is the most suitable storage service.

As mentioned above, EBS provides the lowest-latency access to the data for your EC2 instance since the volume is directly attached to the instance. In addition, the scenario does not require concurrently-accessible storage since they only have one instance.

Hence, the correct answer is EBS.

Storage Gateway is incorrect since this is primarily used to extend your on-premises storage to your AWS Cloud. S3 is incorrect because although this is also highly available and highly scalable, it still does not provide the lowest-latency access to the data, unlike EBS. Remember that S3 does not reside within your VPC by default, which means the data will traverse the public Internet that may result to higher latency.

You can set up a VPC Endpoint for S3 yet still, its latency is greater than that of EBS. EFS is incorrect because the scenario does not require concurrently-accessible storage since the internal application is only hosted in one instance. Although EFS can provide low latency data access to the EC2 instance as compared with S3, the storage service that can provide the lowest latency access is still EBS.

References:

<https://aws.amazon.com/ebs/> <https://aws.amazon.com/efs/faq/>

[Go back to Q168](#)

Answer to Q169: B

[Go back to Q169](#)

Explanation to Q169

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Connecting your current applications to Amazon MQ is easy because it uses industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Using standards means that in most cases, there's no need to rewrite any messaging code when you migrate to AWS.

Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications.

If you are building brand new applications in the cloud, then it is highly recommended that you consider Amazon SQS and Amazon SNS. Amazon SQS and SNS are lightweight, fully managed message queue and topic services that scale almost infinitely and provide simple, easy-to-use APIs. You can use Amazon SQS and SNS to decouple and scale microservices, distributed systems, and serverless applications, and improve reliability.

Hence, Amazon MQ is the correct answer.

Amazon SNS is incorrect because this is more suitable as a pub/sub messaging service instead of a message broker service.

Amazon SQS is incorrect because although this is a fully managed message queuing service, it does not support an extensive list of industry-standard

messaging APIs and protocol, unlike Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

Amazon SWF is incorrect because this is a fully-managed state tracker and task coordinator service and not a messaging service, unlike Amazon MQ, AmazonSQS, and Amazon SNS.

References:

<https://aws.amazon.com/amazon-mq/>

<https://aws.amazon.com/messaging/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sq-sqs-difference-from-amazon-mq-sns>

[Go back to Q169](#)

Answer to Q170: B, D

[Go back to Q170](#)

Explanation to Q170

Amazon EBS provides three volume types to best meet the needs of your workloads: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic.

General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development, and test environments, and boot volumes.

Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance and are designed for I/O intensive applications such

as large relational or NoSQL databases. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types.

Magnetic volumes are ideal for workloads where data are accessed infrequently, and applications where the lowest storage cost is important. Take note that this is a Previous Generation Volume. The latest low-cost magnetic storage types are Cold HDD (sc1) and Throughput Optimized HDD (st1) volumes.

Hence, the correct answers are

1. 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.
2. 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.

The option that says: 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 is incorrect because there is no EBS type called a "Spot volume" however, there is an Instance purchasing option for Spot Instances.

The option that says: Reduced Redundancy Storage volumes offer consistent and low-latency performance and are designed for I/O intensive applications such as large relational or NoSQL databases is incorrect because there is no such thing as Reduced Redundancy Storage volumes. In Amazon S3, there is an obsolete storage type named: Reduced Redundancy Storage (RRS), but not in EBS.

The option that says: 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 is incorrect because SR-IOV is related with Enhanced Networking on Linux and not in EBS.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

[Go back to Q170](#)

Answer to Q171: B

[Go back to Q171](#)

Explanation to Q171

When you create or update a distribution in CloudFront, you can add an origin access identity (OAI) and automatically update the bucket policy to give the origin access identity permission to access your bucket.

Alternatively, you can choose to manually change the bucket policy or change ACLs, which control permissions on individual objects in your bucket.

You can update the Amazon S3 bucket policy using either the AWS Management Console or the Amazon S3 API:- Grant the CloudFront origin access identity the applicable permissions on the bucket.- Deny access to anyone that you don't want to have access using Amazon S3 URLs.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html#private-content-granting-permissions-to-oai>

[Go back to Q171](#)

Answer to Q172: D

[Go back to Q172](#)

Explanation to Q172

Instance metadata is data about your EC2 instance that you can use to configure or manage the running instance. Because your instance metadata is available from your running instance, you do not need to use the Amazon EC2 console or the AWS CLI.

This can be helpful when you're writing scripts to run from your instance. For example, you can access the local IP address of your instance from instance metadata to manage a connection to an external application.

To view the private IPv4 address, public IPv4 address, and all other categories of instance metadata from within a running instance, use the following [URL:http://169.254.169.254/latest/meta-data/](http://169.254.169.254/latest/meta-data/)

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

[Go back to Q172](#)

Answer to Q173: C, E

[Go back to Q173](#)

Explanation to Q173

NA

[Go back to Q173](#)

Answer to Q174: A, C

[Go back to Q174](#)

Explanation to Q174

By default, all Amazon S3 resources such as buckets, objects, and related subresources are private which means that only the AWS account holder (resource owner) that created it has access to the resource. The resource owner can optionally grant access permissions to others by writing an access policy. In S3, you also set the permissions of the object during upload to make it public.

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies.

For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources.

You can also manage the public permissions of your objects during upload. Under Manage public permissions you can grant read access to your objects to the general public (everyone in the world), for all the files that you're uploading. Granting public read access is applicable to a small subset of use cases such as when buckets are used for websites.

Hence, the correct answers are:

1. Grant public read access to the object when uploading it using the S3 Console.
2. Configure the S3 bucket policy to set all objects to public read.

Configuring the ACL of the S3 bucket to set all objects to be publicly readable and writeable is incorrect as ACLs are primarily used to grant basic read/write permissions to AWS accounts and are not suitable for providing public access over the Internet.

Creating an IAM role to set the objects inside the S3 bucket to public read is incorrect. You can create an IAM role and attach it to an EC2 instance in order to retrieve objects from the S3 bucket or add new ones. An IAM Role cannot directly make the S3 objects public or change the permissions of each individual object.

The option that says: Do nothing. Amazon S3 objects are already public by default is incorrect because by default, all the S3 resources are private, so only the AWS account that created the resources can access them.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html>

[Go back to Q174](#)

Answer to Q175: A

[Go back to Q175](#)

Explanation to Q175

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security.

Amazon EC2 is incorrect since this is a compute service, not a storage service.

Amazon Elastic Block Storage is incorrect since EBS is primarily used as a storage of your EC2 instances.

Amazon SQS is incorrect since this is a message queuing service and does not extend your on-premises storage capacity.

Reference:

<http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

[Go back to Q175](#)

Answer to Q176: B

[Go back to Q176](#)

Explanation to Q176

NA

[Go back to Q176](#)

Answer to Q177: D

[Go back to Q177](#)

Explanation to Q177

NA

[Go back to Q177](#)

Answer to Q178: A

[Go back to Q178](#)

Explanation to Q178

The FTP protocol uses TCP via ports 20 and 21. This should be configured in your security groups or in your Network ACL inbound rules. As required by the scenario, you should only allow the individual IP of the client and not the entire network. Therefore, in the Source, the proper CIDR notation should be used. The /32 denotes one IP address and the /0 refers to the entire network.

Notice that the scenario says that you launched the EC2 instances in a newly created VPC with default settings. Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic. Hence, you don't need to explicitly add inbound rules to your Network ACL to allow inbound traffic, if your VPC has a default setting.

The below option is incorrect because although the configuration of the Security Group is valid, the provided Protocol is incorrect. Take note that FTP uses TCP and not UDP.

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

The below option is incorrect because although setting up an inbound Network ACL is valid; the source is invalid since it must be an IPv4 or IPv6 CIDR block. In the provided IP address, the /0 refers to the entire network and not a specific IP address. In addition, the scenario says that the newly created VPC has default settings and by default, the Network ACL allows all traffic. This means that there is no need to configure your Network ACL.

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
The below option is incorrect because, just like Option C, the source is also invalid. Take note that FTP uses TCP and not UDP, which is one of the reasons why this option is wrong. In addition, the scenario says that the newly created VPC has default settings and by default, the Network ACL allows all traffic. This means that there is no need to configure your Network ACL.

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

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

[Go back to Q178](#)

Answer to Q179: B

[Go back to Q179](#)

Explanation to Q179

You can use AWS CloudTrail logs together with server access logs for Amazon S3. CloudTrail logs provide you with detailed API tracking for Amazon S3 bucket-level and object-level operations, while server access

logs for Amazon S3 provide you visibility into object-level operations on your data in Amazon S3.

You can also use CloudTrail logs together with CloudWatch for Amazon S3. CloudTrail integration with CloudWatch Logs delivers S3 bucket-level API activity captured by CloudTrail to a CloudWatch log stream in the CloudWatch log group you specify. You can create CloudWatch alarms for monitoring specific API activity and receive email notifications when the specific API activity occurs.

For this scenario, you can use CloudTrail and the Server Access Logging feature of Amazon S3.

However, the question mentioned that it needs detailed information about every access request sent to the S3 bucket including the referrer and turn-around time information. These two records are not available in CloudTrail which is why the correct answer is to enable server access logging for all required Amazon S3 buckets.

Enabling the Requester Pays option to track access via AWS Billing is incorrect because this action refers to AWS billing and not for logging.

Enabling Amazon S3 Event Notifications for PUT and POST is incorrect because we are looking for a logging solution and not an event notification.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html#cloudtrail-logging-vs-server-logs>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html>

[Go back to Q179](#)

Answer to Q180: A

[Go back to Q180](#)

Explanation to Q180

You require an EC2 instance that is the most cost-effective among other types. In addition, the application it will host is designed to gracefully recover in case of instance failures.

In terms of cost-effectiveness, Spot and Reserved instances are the top options. And since the application can gracefully recover from instance failures, the Spot instance is the best option for this case as it is the cheapest type of EC2 instance.

Remember that when you use Spot Instances, there will be interruptions. Amazon EC2 can interrupt your Spot Instance when the Spot price exceeds your maximum price, when the demand for Spot Instances rise, or when the supply of Spot Instances decreases. This makes Spot Instances the correct answer.

Reserved instances are incorrect because although you could also use reserved instances to save costs, it entails a commitment of 1-year or 3-year terms of usage. Since your processes only run periodically, you won't be able to maximize the discounted price of using reserved instances.

Dedicated instances and On-Demand instances are also incorrect because Dedicated and on-demand instances are not a cost-effective solution to use for your application.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html>

[Go back to Q180](#)

Answer to Q181: D, E

[Go back to Q181](#)

Explanation to Q181

AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

This file serves as the single source of truth for your cloud environment. AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications.

Hence, the correct answers are:

1. Enables modeling, provisioning, and version-controlling of your entire AWS infrastructure
2. Allows you to model your entire infrastructure in a text file

The option that says: Provides highly durable and scalable data storage is incorrect because CloudFormation is not a data storage service.

The option that says: A storage location for the code of your application is incorrect because CloudFormation is not used to store your application code. You must use CodeCommit as a code repository and not CloudFormation.

The option that says: Using CloudFormation itself is free, including the AWS resources that have been created is incorrect because although the use of CloudFormation service is free, you must pay the AWS resources that you created.

References:

<https://aws.amazon.com/cloudformation/>

<https://aws.amazon.com/cloudformation/faqs/>

[Go back to Q181](#)

Answer to Q182: A

[Go back to Q182](#)

Explanation to Q182

In this question, you should take note of the two keywords/phrases: "file operation" and "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time. Amazon EFS provides the scale and performance required for big data applications that require high throughput to compute nodes coupled with read-after-write consistency and low-latency file operations.

Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

EBS is incorrect because it does not allow concurrent connections from multiple EC2 instances hosted on multiple AZs and it does not store data redundantly across multiple AZs by default, unlike EFS. S3 is incorrect because although it can handle concurrent connections from multiple EC2 instances, it does not have the ability to provide low-latency file operations, which is required in this scenario.

Glacier is incorrect because this is an archiving storage solution and is not applicable in this scenario.

References:

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>
<https://aws.amazon.com/efs/faq/>

[Go back to Q182](#)

Answer to Q183: A

[Go back to Q183](#)

Explanation to Q183

DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

Using DynamoDB Auto Scaling is the best answer. DynamoDB Auto Scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf.

Integrating an Application Load Balancer with your DynamoDB table is incorrect because an Application Load Balancer is not suitable to be used with DynamoDB and in addition, this will not increase the throughput of your DynamoDB table.

Adding the DynamoDB table to an Auto Scaling Group is incorrect because you usually put EC2 instances on an Auto Scaling Group, and not a DynamoDB table.

Creating an SQS queue in front of the DynamoDB table is incorrect because this is not a design principle for high throughput DynamoDB table. Using SQS is for handling queuing and polling the request. This will not increase the throughput of DynamoDB which is required in this situation.

Reference:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

[Go back to Q183](#)

Answer to Q184: B

[Go back to Q184](#)

Explanation to Q184

NA

[Go back to Q184](#)

Answer to Q185: B

[Go back to Q185](#)

Explanation to Q185

In this scenario, you need to enable Cross-Region Replication to ensure that your S3 bucket would not be affected even if there is an outage in one of the Availability Zones or a regional service failure in us-east-1. When you upload your data in S3, your objects are redundantly stored on multiple devices across multiple facilities within the region only, where you created the bucket. Thus, if there is an outage on the entire region, your S3 bucket will be unavailable if you do not enable Cross-Region Replication, which should make your data available to another region.

Note that an Availability Zone (AZ) is more related with Amazon EC2 instances rather than Amazon S3 so if there is any outage in the AZ, the S3 bucket is usually not affected but only the EC2 instances deployed on that zone.

Hence, the correct answer is: Enable Cross-Region Replication.

The option that says: Copy the S3 bucket to an EBS-backed EC2 instance is incorrect because EBS is not as durable as Amazon S3. Moreover, if the Availability Zone where the volume is hosted goes down then the data will also be inaccessible.

The option that says: Create a Lifecycle Policy to regularly backup the S3 bucket to Amazon Glacier is incorrect because Glacier is primarily used for data archival. You also need to replicate your data to another region for better durability.

The option that says: Create a new S3 bucket in another region and configure Cross-Account Access to the bucket located in us-east-1 is incorrect because Cross-Account Access in Amazon S3 is primarily used if you want to grant access to your objects to another AWS account, and not just to another AWS Region.

For example, Account MANILA can grant another AWS account (Account CEBU) permission to access its resources such as buckets and objects. S3 Cross-Account Access does not replicate data from one region to another. A better solution is to enable Cross-Region Replication (CRR) instead.

References:

<https://aws.amazon.com/s3/faqs/https://aws.amazon.com/s3/features/application/>

[Go back to Q185](#)

Answer to Q186: A

[Go back to Q186](#)

Explanation to Q186

NA

[Go back to Q186](#)

Answer to Q187: D

[Go back to Q187](#)

Explanation to Q187

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

Athena is serverless, so there is no infrastructure to set up or manage, and you pay only for the queries you run. Athena scales automatically executing queries in parallel, so results are fast, even with large datasets and complex queries.

Athena helps you analyze unstructured, semi-structured, and structured data stored in Amazon S3. Examples include CSV, JSON, or columnar data

formats such as Apache Parquet and Apache ORC. You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena.

Hence, the most cost-effective and appropriate answer in this scenario is the option that says: To be able to run SQL queries, use Amazon Athena to analyze the export data file in S3. The rest of the options are all incorrect because it is not necessary to set up a database to be able to analyze the CSV export file. You can use a cost-effective option (AWS Athena), which is a serverless service that enables you to pay only for the queries you run.

Reference:

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

[Go back to Q187](#)

Answer to Q188: B

[Go back to Q188](#)

Explanation to Q188

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

In the scenario given, we can utilize AWS Config to check for compliance on the password policy by configuring the Config rule to check the IAM_PASSWORD_POLICY on an account. Additionally, because Config integrates with AWS Organizations, we can improve the set up to aggregate compliance information across accounts to a central dashboard.

Hence, the correct answer is: Configure AWS Config to trigger an evaluation that will check the compliance for a user's password periodically.

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 is incorrect because this setup will just give you the name of the users who have made changes to their respective passwords. It will not give you the ability to check whether their passwords have met the required minimum length.

Create a Scheduled Lambda function that will run a custom script to check compliance against changes made to the passwords periodically is a valid solution but still incorrect. AWS Config is already integrated with AWS Lambda. You don't have to create and manage your own Lambda function. You just must define a Config rule where you will check compliance, and Lambda will process the evaluation. Moreover, you can't directly create a scheduled function by using Lambda itself. You must create a rule in AWS CloudWatch Events to run the Lambda functions on the schedule that you define.

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 is incorrect because this setup will just alert you whenever a user changes his password. Sure, you'll have information about who made changes, but that is not enough to check whether it complies with the required minimum password length. This can be easily done in AWS Config.

References:

<https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html>

<https://aws.amazon.com/config/>

[Go back to Q188](#)

Answer to Q189: B

[Go back to Q189](#)

Explanation to Q189

NA

[Go back to Q189](#)

Answer to Q190: B

[Go back to Q190](#)

Explanation to Q190

In this scenario, you can 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.

You can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances using Amazon CloudWatch alarm actions. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

The option that says: 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 is incorrect because you can't create an alarm in Amazon SNS.

The options that say: 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 and 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 are incorrect because Flow Logs are used in VPC and not on specific EC2 instance.

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

[Go back to Q190](#)

Answer to Q191: D

[Go back to Q191](#)

Explanation to Q191

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS.

You can create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. With this, you can deploy an exact copy of your AWS architecture, along with all the AWS resources which are hosted in one region to another.

Hence, the correct answer is AWS CloudFormation.

Amazon LightSail is incorrect because you can't use this to duplicate your resources in your VPC. You must use CloudFormation instead.

Amazon SQS and Amazon SNS are both incorrect because SNS and SQS are just messaging services.

References:

[<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-cli-creating-stack.html>](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

[Go back to Q191](#)

Answer to Q192: D

[Go back to Q192](#)

Explanation to Q192

AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services. Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources.

AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)aware applications in the cloud. It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

Every AWS resource is owned by an AWS account, and permissions to create or access the resources are governed by permissions policies. An

account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles), and some services (such as AWS Lambda) also support attaching permissions policies to resources.

The following resource policy example allows all ds calls if the resource contains the directory ID "d-1234567890".

```
{ "Version":"2012-10-17", "Statement": [ { "Sid":"VisualEditor0", "Effect":"Allow", "Action": [ "ds:*" ], "Resource": "arn:aws:ds:us-east-1:123456789012:directory/d-1234567890" }, { "Effect":"Allow", "Action": [ "ec2:*" ], "Resource": "*" } ] }
```

Hence, the correct answer is the option that says: Allows all AWS Directory Service (ds) calls as long as the resource contains the directory ID: d-1234567890.

The option that says: Allows all AWS Directory Service (ds) calls as long as the resource contains the directory ID: DirectoryTechradio1234 is incorrect because DirectoryTechradio1234 is the Statement ID (SID) and not the Directory ID.

The option that says: Allows all AWS Directory Service (ds) calls if the resource contains the directory ID: 987654321012 is incorrect because the numbers: 987654321012 is the Account ID and not the Directory ID.

The option that says: Allows all AWS Directory Service (ds) calls if the resource contains the directory name of: DirectoryTechradio1234 is incorrect because DirectoryTechradio1234 is the Statement ID (SID) and not the Directory name.

References:

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/IAM_Auth_Access_IdentityBased.html

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/IAM_Auth_Access_Overview.html

[Go back to Q192](#)

Answer to Q193: A, C

[Go back to Q193](#)

Explanation to Q193

Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance terminates, which could occur through a web services command, by running "shutdown -h", or through instance failure. When you stop an instance, AWS shuts it down but don't charge hourly usage for a stopped instance or data transfer fees, but AWS does charge for the storage of any Amazon EBS volumes.

Hence, a running EC2 Instance and EBS Volumes attached to stopped EC2 Instances are the right answers and conversely, a stopped On-Demand EC2 Instance is incorrect as there is no charge for a terminated EC2 instance that you have shut down.

Using Amazon VPC is incorrect because there are no additional charges for creating and using the VPC itself. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges.

Public Data Set is incorrect since Amazon stores the data sets at no charge to the community and, as with all AWS services, you pay only for the compute and storage you use for your own applications.

References:

<https://aws.amazon.com/cloudtrail/><https://aws.amazon.com/vpc/faqs>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html>

[Go back to Q193](#)

Answer to Q194: C

[Go back to Q194](#)

Explanation to Q194

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads.

Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.

Hence, the correct answer is: Amazon S3 for storing the application log files and Amazon Elastic MapReduce for processing the log files.

The option that says: Amazon S3 Glacier for storing the application log files and Spot EC2 Instances for processing them is incorrect as Amazon S3 Glacier is used for data archive only.

The option that says: A single On-Demand Amazon EC2 instance for both storing and processing the log files is incorrect as an EC2 instance is not a recommended storage service. In addition, Amazon EC2 does not have a built-in data processing engine to process large amounts of data.

The option that says: Amazon S3 Glacier Deep Archive for storing the application log files and AWS ParallelCluster for processing the log files is incorrect because the long retrieval time of Amazon S3 Glacier Deep Archive makes this option unsuitable.

Moreover, AWS ParallelCluster is just an AWS-supported open-source cluster management tool that makes it easy for you to deploy and manage High-Performance Computing (HPC) clusters on AWS. ParallelCluster uses a simple text file to model and provision all the resources needed for your HPC applications in an automated and secure manner.

References:

<http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

<https://aws.amazon.com/hpc/parallelcluster/>

[Go back to Q194](#)

Answer to Q195: B

[Go back to Q195](#)

Explanation to Q195

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. You are charged for creating and using a NAT gateway in your account.

NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply. NAT gateways are not supported for IPv6 traffic use an egress-only internet gateway instead.

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. The Elastic IP address cannot be changed once you associate it with the NAT Gateway.

After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet. Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone. You have a limit on the number of NAT gateways you can create in an Availability Zone.

Hence, the correct answer is to 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.

Deploying the web and application tier instances to a private subnet and then allocating an Elastic IP address to each EC2 instance is incorrect because an Elastic IP address is just a static, public IPv4 address. In this scenario, you must use a NAT Gateway instead.

Deploying a NAT gateway in the private subnet and adding a route to it from the public subnet where the web and application tiers are hosted is incorrect because you have to deploy a NAT gateway in the public subnet instead and not on a private one.

Deploying the web and application tier instances to a public subnet and then allocating an Elastic IP address to each EC2 instance is incorrect because having an EIP address is irrelevant as it is only a static, public IPv4 address. Moreover, you should deploy the web and application tier in the private subnet instead of a public subnet to make it inaccessible from the Internet and then just add a NAT Gateway to allow outbound Internet connection.

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

[Go back to Q195](#)

Answer to Q196: C

[Go back to Q196](#)

Explanation to Q196

You require an instance that will be used not as a primary server but as a spare compute resource to augment the transcoding process of your application. These instances should also be terminated once the backlog has been significantly reduced. In addition, the scenario mentions that if the current process is interrupted, the video can be transcoded by another instance based on the queuing system. This means that the application can gracefully handle an unexpected termination of an EC2 instance, like in the event of a Spot instance termination when the Spot price is greater than your set maximum price. Hence, an Amazon EC2 Spot instance is the best and cost-effective option for this scenario. Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. EC2 Spot enables you to optimize your costs on the AWS cloud and scale your application's throughput up to 10X for the same budget. By simply selecting Spot when launching EC2 instances, you can save up-to 90% on On-Demand prices. The only difference between On-Demand instances and Spot Instances is that Spot instances can be interrupted by EC2 with two minutes of notification when the EC2 needs the capacity back. You can specify whether Amazon EC2 should hibernate, stop, or terminate Spot Instances when they are interrupted. You can choose the interruption behavior that meets your needs.

Take note that there is no "bid price" anymore for Spot EC2 instances since March 2018. You simply must set your maximum price instead.

Reserved instances and Dedicated instances are incorrect as both do not act as spare compute capacity.

On-demand instances is a valid option, but a Spot instance is much cheaper than On-Demand.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-spot-instances-work.html>

<https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing>

[Go back to Q196](#)

Answer to Q197: A, D

[Go back to Q197](#)

Explanation to Q197

Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a route table. Otherwise, the subnet is implicitly associated with the main route table.

A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table. You can optionally associate a route table with an internet gateway or a virtual private gateway (gateway route table). This enables you to specify routing rules for inbound traffic that enters your VPC through the gateway.

Be sure that the subnet route table also has a route entry to the internet gateway. If this entry doesn't exist, the instance is in a private subnet and is inaccessible from the internet.

In cases where your EC2 instance cannot be accessed from the Internet (or vice versa), you usually must check two things:- Does it have an EIP or public IP address?- Is the route table properly configured?

Below are the correct answers:

1. Amazon EC2 instance does not have a public IP address associated with it.
2. The route table is not configured properly to send traffic from the EC2 instance to the Internet through the Internet gateway.

The option that says: The Amazon EC2 instance is not a member of the same Auto Scaling group is incorrect since Auto Scaling Groups do not affect Internet connectivity of EC2 instances.

The option that says: The Amazon EC2 instance doesn't have an attached Elastic Fabric Adapter (EFA) is incorrect because the Elastic Fabric Adapter is just a network device that you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications. EFA enables you to achieve the application performance of an on-premises HPC cluster, with the scalability, flexibility, and elasticity provided by AWS. However, this component is not required for your EC2 instance to access the public Internet.

The option that says: The route table is not configured properly to send traffic from the EC2 instance to the Internet through the customer gateway (CGW) is incorrect since CGW is used when you are setting up a VPN. The correct gateway should be an Internet gateway.

References:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario_2.html

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

[Go back to Q197](#)

Answer to Q198: A, C

[Go back to Q198](#)

Explanation to Q198

The correct options are:- Go to the AWS Reserved Instance Marketplace and sell the Reserved instances.- Terminate the Reserved instances as soon as possible to avoid getting billed at the on-demand price when it expires.

The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in terms of lengths and pricing options.

For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity.

Stopping the Reserved instances as soon as possible is incorrect because a stopped instance can still be restarted. Take note that when a Reserved Instance expires, any instances that were covered by the Reserved Instance are billed at the on-demand price which costs significantly higher.

Since the application is already decommissioned, there is no point of keeping the unused instances. It is also possible that there are associated Elastic IP addresses, which will incur charges if they are associated with stopped instances.

Contacting AWS to cancel your AWS subscription is incorrect as you don't need to close your AWS account.

Going to the Amazon.com online shopping website and selling the Reserved instances is incorrect as you must use AWS Reserved Instance Marketplace to sell your instances.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

[Go back to Q198](#)

Answer to Q199: B

[Go back to Q199](#)

Explanation to Q199

You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.

Active-Active Failover. Use this failover configuration when you want all your resources to be available most of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or

latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.

Active-Passive Failover. Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

Configuring an Active-Passive Failover with Weighted Records and configuring an Active-Passive Failover with Multiple Primary and Secondary Resources are incorrect because an Active-Passive Failover is mainly used when you want a primary resource or group of resources to be available most of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable.

In this scenario, all your resources should be available all the time as much as possible which is why you have to use an Active-Active Failover instead.

Configuring an Active-Active Failover with One Primary and One Secondary Resource is incorrect because you cannot set up an Active-Active Failover with One Primary and One Secondary Resource. Remember that an Active-Active Failover uses all available resources all the time without a primary nor a secondary resource.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-configuring.html>

[Go back to Q199](#)

Answer to Q200: C

[Go back to Q200](#)

Explanation to Q200

Amazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions with one caveat: if you make a HEAD or GET request to the key name (to find if the object exists) before creating the object, Amazon S3 provides eventual consistency for read-after-write.

Amazon S3 offers eventual consistency for overwrite PUTS and Deletes in all regions.

Updates to a single key are atomic. For example, if you PUT to an existing key, a subsequent read might return the old data or the updated data, but it will never return corrupted or partial data. This usually happens if your application is using parallel requests on the same object.

Amazon S3 achieves high availability by replicating data across multiple servers within Amazon's data centers. If a PUT request is successful, your data is safely stored. However, information about the changes must replicate across Amazon S3, which can take some time, and so you might observe the following behaviors:

- A process writes a new object to Amazon S3 and immediately lists keys within its bucket. Until the change is fully propagated, the object might not appear in the list.
- A process replaces an existing object and immediately attempts to read it. Until the change is fully propagated, Amazon S3 might return the prior data.

- A process deletes an existing object and immediately attempts to read it. Until the deletion is fully propagated, Amazon S3 might return the deleted data.
- A process deletes an existing object and immediately lists keys within its bucket. Until the deletion is fully propagated, Amazon S3 might list the deleted object.

Amazon S3's support for parallel requests means you can scale your S3 performance by the factor of your compute cluster, without making any customizations to your application. Amazon S3 does not currently support Object Locking. If two PUT requests are simultaneously made to the same key, the request with the latest timestamp wins. If this is an issue, you will need to build an object-locking mechanism into your application.

Updates are key-based; there is no way to make atomic updates across keys. For example, you cannot make the update of one key dependent on the update of another key unless you design this functionality into your application.

Hence, the correct answer is the option that says: The data analytics application is designed to fetch objects from the S3 bucket using parallel requests.

The option that says: The data analytics application is designed to fetch parts of objects from the S3 bucket using a range header is incorrect because using a Range header is primarily used to retrieve an object in parts and is unlikely the root cause on why the application is intermittently getting old data. Using the Range HTTP header in a GET request, you can retrieve a specific range of bytes in an object stored in Amazon S3. With this, you can resume fetching other parts of the object whenever your application is ready. This resumable download is useful when you need only portions of your object data. It is also useful where network connectivity is poor, and you need to react to failures.

The option that says: The data analytics application is designed to use atomic updates across object keys is incorrect because the update

operations are key-based which means that there is no way to make atomic updates across keys. Hence, this is not the root cause of this issue.

The option that says: The data analytics application is designed to update its data with an object-locking mechanism is incorrect because an object-locking mechanism will safeguard the application from the issue of getting obsolete data and not the other way around. Moreover, Amazon S3 does not currently support Object Locking for concurrent updates. Take note that this is different from the Amazon S3 Object Lock feature which prevents an object from being deleted or overwritten for a fixed amount of time or indefinitely. The scenario mentioned here is about two or more clients that are concurrently accessing and updating the same object at the same time. An "Object-locking" mechanism is a system that "locks" the very first update request to the S3 object and blocks any concurrent update requests to the same object.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html>

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectGET.html>

[Go back to Q200](#)

Answer to Q201: C

[Go back to Q201](#)

Explanation to Q201

Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied immediately regardless of any higher-numbered rule that may contradict it.

We have 3 rules here:
1. Rule 100 permits all traffic from any source.
2. Rule 101 denies all traffic coming from 110.238.109.373. The Default Rule (*) denies all traffic from any source.

The Rule 100 will first be evaluated. If there is a match, then it will allow the request. Otherwise, it will then go to Rule 101 to repeat the same process until it goes to the default rule. In this case, when there is a request from 110.238.109.37, it will go through Rule 100 first. As Rule 100 says it will permit all traffic from any source, it will allow this request and will not further evaluate Rule 101 (which denies 110.238.109.37) nor the default rule.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[Go back to Q201](#)

Answer to Q202: D

[Go back to Q202](#)

Explanation to Q202

In this scenario, the best way to accomplish the requirement is to simply configure the lifecycle configuration rules on the Amazon S3 bucket to purge the transaction logs after a month.

Lifecycle configuration enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects.

These actions can be classified as follows:

1. Transition actions: In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
2. Expiration actions: In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Adding a new bucket policy on the Amazon S3 bucket is incorrect as it does not provide a solution to any of your needs in this scenario. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it.

Creating a new IAM policy for the Amazon S3 bucket that automatically deletes the logs after a month is incorrect because IAM policies are primarily used to specify what actions are allowed or denied on your S3 buckets. You cannot configure an IAM policy to automatically purge logs for you in any way.

Enabling CORS on the Amazon S3 bucket which will enable the automatic monthly deletion of data is incorrect. CORS allows client web applications that are loaded in one domain to interact with resources in a different domain.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

[Go back to Q202](#)

Answer to Q203: A

[Go back to Q203](#)

Explanation to Q203

In this scenario, the best option is to group the set of users in an IAM Group and then apply a policy with the required access to the Amazon S3 bucket. This will enable you to easily add, remove, and manage the users instead of manually adding a policy to each of the 100 IAM users.

Creating a new policy and applying it to multiple IAM users using a shell script is incorrect because you need a new IAM Group for this scenario and not assign a policy to each user via a shell script. This method can save you time but afterwards, it will be difficult to manage all 100 users that are not contained in an IAM Group.

Creating a new S3 bucket access policy with unlimited access for each IAM user is incorrect because you need a new IAM Group and the method is also time-consuming.

Creating a new IAM role and adding each user to the IAM role is incorrect because you need to use an IAM Group and not an IAM role.

Reference:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

[Go back to Q203](#)

Answer to Q204: A

[Go back to Q204](#)

Explanation to Q204

Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a durable, highly-scalable, reliable, and low-latency data storage infrastructure at very low costs. Amazon S3 provides customers with a highly durable storage infrastructure. Versioning offers an additional level of protection by providing a means of recovery when

customers accidentally overwrite or delete objects. Remember that the scenario requires a durable storage for static content. These two keywords are referring to S3, since it is highly durable and suitable for storing static content.

Hence, Amazon S3 is the correct answer. Amazon EBS volume is incorrect because this is not as durable compared with S3. In addition, it is best to store the static contents in S3 rather than EBS.

Amazon EC2 instance store is incorrect because it is not suitable - the data it holds will be wiped out immediately once the EC2 instance is restarted.

Amazon RDS instance is incorrect because an RDS instance is just a database and not suitable for storing static content. By default, RDS is not durable, unless you launch it to be in Multi-AZ deployments configuration.

Reference:

<https://aws.amazon.com/s3/faqs/>

<https://d1.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=24>

[Go back to Q204](#)

Answer to Q205: A, D

[Go back to Q205](#)

Explanation to Q205

By working with Amazon EC2 to manage your instances from the moment you launch them through their termination, you ensure that your customers have the best possible experience with the applications or sites that you host on your instances. The following illustration represents the

transitions between instance states. Notice that you can't stop and start an instance store-backed instance.

Below are the valid EC2 lifecycle instance states:

1. pending - The instance is preparing to enter the running state. An instance enters the pending state when it launches for the first time, or when it is restarted after being in the stopped state.
2. running - The instance is running and ready for use.
3. stopping - The instance is preparing to be stopped. Take note that you will not be billed if it is preparing to stop however, you will still be billed if it is just preparing to hibernate.
4. stopped - The instance is shut down and cannot be used. The instance can be restarted at any time.
5. shutting-down - The instance is preparing to be terminated.
6. terminated - The instance has been permanently deleted and cannot be restarted. Take note that Reserved Instances that applied to terminated instances are still billed until the end of their term according to their payment option.

The option that says: You will be billed when your On-Demand instance is preparing to hibernate with a stopping state is correct because when the instance state is stopping, you will not be billed if it is preparing to stop however, you will still be billed if it is just preparing to hibernate.

The option that says: You will be billed when your Reserved instance is in terminated state is correct because Reserved Instances that applied to terminated instances are still billed until the end of their term according to their payment option.

The option that says: You will be billed when your On-Demand instance is in pending state is incorrect because you will not be billed if your instance is in pending state.

The option that says: You will be billed when your Spot instance is preparing to stop with a stopping state is incorrect because you will not be billed if your instance is preparing to stop with a stopping state.

The option that says: You will not be billed for any instance usage while an instance is not in the running state is incorrect because the statement is not entirely true. You can still be billed if your instance is preparing to hibernate with a stopping state.

References:

<https://github.com/awsdocs/amazon-ec2-user-guide/pull/45>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

[Go back to Q205](#)

Answer to Q206: C

[Go back to Q206](#)

Explanation to Q206

By default, a "default subnet" of your VPC is a public subnet, because the main route table sends the subnet's traffic that is destined for the internet to the internet gateway. You can make a default subnet into a private subnet by removing the route from the destination 0.0.0.0/0 to the internet gateway. However, if you do this, any EC2 instance running in that subnet can't access the internet.

Instances that you launch into a default subnet receive both a public IPv4 address and a private IPv4 address, and both public and private DNS hostnames. Instances that you launch into a nondefault subnet in a default VPC don't receive a public IPv4 address or a DNS hostname. You can change your subnet's default public IP addressing behavior.

By default, nondefault subnets have the IPv4 public addressing attribute set to false, and default subnets have this attribute set to true. An exception is a nondefault subnet created by the Amazon EC2 launch instance wizard—the wizard sets the attribute to true.

In this scenario, it is possible that the fifth EC2 instance launched in a nondefault subnet doesn't have a public IP address or an Elastic IP address, just like the first 4 instances.

Associating an Elastic IP address to the fifth EC2 instance is correct because the fifth instance does not have a public IP address since it was deployed on a nondefault subnet. The other 4 instances are accessible over the Internet because they each have an Elastic IP address attached, unlike the last instance which only has a private IP address. An Elastic IP address is a public IPv4 address, which is reachable from the Internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the Internet.

Including the fifth EC2 instance to the Placement Group of the other four EC2 instances and enabling Enhanced Networking is incorrect because Placement Groups is primarily used to determine how your instances are placed on the underlying hardware while Enhanced Networking, on the other hand, is for providing high-performance networking capabilities using single root I/O virtualization (SR-IOV) on supported EC2 instance types.

Setting up a NAT gateway to allow access to the fifth EC2 instance is incorrect because you do not need a NAT Gateway nor a NAT instance in this scenario considering that the instances are already in public subnet. Remember that a NAT Gateway or a NAT instance is primarily used to

enable instances in a private subnet to connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances.

Enabling AWS Transfer for SFTP to allow the incoming traffic to the fifth EC2 Instance is incorrect because AWS Transfer for SFTP (AWS SFTP) is simply a fully managed AWS service that enables you to transfer files over Secure File Transfer Protocol (SFTP), into and out of Amazon Simple Storage Service (Amazon S3) storage. This service is not related to EC2 instances at all.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/default-vpc.html>

<https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-for-sftp.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>

[Go back to Q206](#)

Answer to Q207: D

[Go back to Q207](#)

Explanation to Q207

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

Amazon CloudFront is incorrect because this is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. It does not provide any deployment capability for your custom applications unlike Elastic Beanstalk.

AWS CloudFormation is incorrect because although this service provides deployment capabilities, you will still have to design a custom template that contains the required AWS resources for your application needs. Hence, this will require more time to complete instead of just directly using Elastic Beanstalk.

AWS CodeCommit is incorrect because although you can upload your NodeJS code in AWS CloudCommit, this service is just a fully-managed source control service that hosts secure Git-based repositories and hence, it does not provide a way to deploy or manage your applications in AWS.

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

[Go back to Q207](#)

Answer to Q208: B

[Go back to Q208](#)

Explanation to Q208

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Building applications from individual components that each perform a discrete function improves scalability and reliability and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a

cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available.

The number of messages in your Amazon SQS queue does not solely define the number of instances needed. In fact, the number of instances in the fleet can be driven by multiple factors, including how long it takes to process a message and the acceptable amount of latency (queue delay). The solution is to use a backlog per instance metric with the target value being the acceptable backlog per instance to maintain.

You can calculate these numbers as follows:

1. Backlog per instance: To determine your backlog per instance, start with the Amazon SQS metric `ApproximateNumberOfMessages` to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the `InService` state, to get the backlog per instance.
2. Acceptable backlog per instance: To determine your target value, first calculate what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.
3. To illustrate with an example, let's say that the current `ApproximateNumberOfMessages` is 1500 and the fleet's running capacity is 10. If the average processing time is 0.1 seconds for each message and the longest acceptable latency is 10 seconds then the acceptable backlog per instance is $10 / 0.1$, which equals 100. This means that 100 is the target value for your target tracking policy. Because the backlog per instance is currently at 150 ($1500 / 10$), your fleet scales out by five instances to maintain proportion to the target value.

Hence, the correct answer is: Use an Amazon SQS queue to decouple the application components and scale-out the EC2 instances based upon the `ApproximateNumberOfMessages` metric in Amazon CloudWatch.

Replacing the Auto Scaling group with a cluster placement group to achieve a low-latency network performance necessary for tightly-coupled node-to-node communication is incorrect because although it is true that a cluster placement group allows you to achieve a low-latency network performance, you still need to use Auto Scaling for your architecture to add more EC2 instances.

Using larger instances for your application with an attached Elastic Fabric Adapter (EFA) is incorrect because using a larger EC2 instance would not prevent data from being lost in case of a larger spike. You can take advantage of the durability and elasticity of SQS to keep the messages available for consumption by your instances. Elastic Fabric Adapter (EFA) is simply a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS.

Setting up Amazon Aurora Serverless for on-demand, auto-scaling configuration of your EC2 Instances and also enabling Amazon Aurora Parallel Query feature for faster analytical queries over your current data is incorrect because although the Amazon Aurora Parallel Query feature provides faster analytical queries over your current data, Amazon Aurora Serverless is an on-demand, auto-scaling configuration for your database, and NOT for your EC2 instances. This is an auto-scaling configuration for your Amazon Aurora database and not for your compute services.

References:

<https://aws.amazon.com/sqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>

[Go back to Q208](#)

Answer to Q209: D

[Go back to Q209](#)

Explanation to Q209

Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPCs VPN solution.

You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your customer gateway on the remote side of the VPN connection. If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks.

With AWS Site-to-Site VPN, you can connect to an Amazon VPC in the cloud the same way you connect to your branches. AWS Site-to-Site VPN establishes secure and private sessions with IP Security (IPSec) and Transport Layer Security (TLS) tunnels.

Hence, the correct answer is the option that says: 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 since one of the main advantages of having a VPN connection is that you will be able to connect your Amazon VPC to other remote networks securely.

The option that says: It provides a cost-effective, hybrid connection from your VPC to your on-premises data centers which bypasses the public Internet is incorrect because although it is true that a VPN provides a cost-effective, hybrid connection from your VPC to your on-premises data centers, it certainly does not bypass the public Internet. A VPN connection goes through the public Internet, unlike the AWS Direct Connect connection which has a direct and dedicated connection to your on-premises network.

The option that says: It provides a networking connection between two VPCs which enables you to route traffic between them using private IPv4 addresses or IPv6 addresses is incorrect because this describes VPC Peering and not a VPN connection.

The option that says: It enables you to establish a private and dedicated network connection between your network and your VPC is incorrect because this is the advantage of an AWS Direct Connect connection and not a VPN.

References:

<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/software-vpn-network-to-amazon.html>

[Go back to Q209](#)

Answer to Q210: C

[Go back to Q210](#)

Explanation to Q210

In this scenario, you can use lifecycle policies in S3 to automatically move obsolete data to Glacier.

Lifecycle configuration in Amazon S3 enables you to specify the lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

1. Transition actions: In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
2. Expiration actions: In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

Using an EC2 instance and a scheduled job to transfer the obsolete data from their S3 location to Amazon S3 Glacier is incorrect because you don't need to create a scheduled job in EC2 as you can just simply use the lifecycle policy in S3. Using Amazon SQS and Amazon SWF are incorrect as SQS and SWF are not storage services.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://aws.amazon.com/blogs/aws/archive-s3-to-glacier/>

[Go back to Q210](#)

Answer to Q211: A

[Go back to Q211](#)

Explanation to Q211

The scenario requires a storage type for a relational database with a high IOPS performance. For these scenarios, SSD volumes are more suitable to use instead of HDD volumes. Remember that the dominant performance attribute of SSD is IOPS while HDD is Throughput.

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has small, random I/O operations or large, sequential I/O operations.

Since the requirement is 30,000 IOPS, you must use an EBS type of Provisioned IOPS SSD. This provides sustained performance for mission-critical low-latency workloads. Hence, EBS Provisioned IOPS SSD (io1) is the correct answer.

EBS Throughput Optimized HDD (st1) and EBS Cold HDD (sc1) are incorrect because these are HDD volumes which are more suitable for large streaming workloads rather than transactional database workloads.

EBS General Purpose SSD (gp2) is incorrect because although a General Purpose SSD volume can be used for this scenario, it does not provide the high IOPS required by the application, unlike the Provisioned IOPS SSD volume.

Reference:

<https://aws.amazon.com/ebs/details/> Check out this Amazon EBS

[Go back to Q211](#)

Answer to Q212: D, E

[Go back to Q212](#)

Explanation to Q212

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

For the MySQL, MariaDB, PostgreSQL, and Oracle database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

When you create a read replica for Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle, Amazon RDS sets up a secure communications channel using public-key encryption between the source DB instance and the read replica, even when replicating across regions. Amazon RDS establishes any AWS security configurations such as adding security group entries needed to enable the secure channel.

You can also create read replicas within a Region or between Regions for your Amazon RDS for MySQL, MariaDB, PostgreSQL, and Oracle database instances encrypted at rest with AWS Key Management Service (KMS). Hence, the correct answers are:- It elastically scales out beyond the capacity constraints of a single DB instance for read-heavy database workloads.- Provides asynchronous replication and improves the performance of the primary database by taking read-heavy database workloads from it.

The option that says: Allows both read and write operations on the read replica to complement the primary database is incorrect as Read Replicas are primarily used to offload read-only operations from the primary database instance. By default, you can't do a write operation to your Read Replica.

The option that says: Provides synchronous replication and automatic failover in the case of Availability Zone service failures is incorrect as this is a benefit of Multi-AZ and not of a Read Replica. Moreover, Read Replicas provide an asynchronous type of replication and not synchronous replication.

The option that says: It enhances the read performance of your primary database by increasing its IOPS and accelerates its query processing via AWS Global Accelerator is incorrect because Read Replicas do not do anything to upgrade or increase the read throughput on the primary DB instance per se, but it provides a way for your application to fetch data from replicas. In this way, it improves the overall performance of your entire database-tier (and not just the primary DB instance).

It doesn't increase the IOPS nor use AWS Global Accelerator to accelerate the compute capacity of your primary database. AWS Global Accelerator is a networking service, not related to RDS, that direct user traffic to the nearest application endpoint to the client, thus reducing internet latency and jitter. It simply routes the traffic to the closest edge location via Anycast.

References:

<https://aws.amazon.com/rds/details/read-replicas/>

<https://aws.amazon.com/rds/features/multi-az/>

[Go back to Q212](#)

Answer to Q213: B

[Go back to Q213](#)

Explanation to Q213

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration.

To create a bastion host, you can create a new EC2 instance which should only have a security group from a IP address for maximum security. Since the cost is also considered in the question, you should choose a small instance for your host. By default, t2.micro instance is used by AWS, but you can change these settings during deployment.

Setting up a large EC2 instance and a security group which only allows access on port 22 via your IP address is incorrect because you don't need to provision a large EC2 instance to run a single bastion host. At the same time, you are looking for the cheapest solution possible.

The options that say: Set up a large EC2 instance and a security group which only allows access on port 22 and Set up a small EC2 instance and a security group which only allows access on port 22 are both incorrect because you did not set your specific IP address to the security group rules, which possibly means that you publicly allow traffic from all sources in your security group.

This is wrong as you should only be the one to have access to the bastion host.

References:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/>

[Go back to Q213](#)

Answer to Q214: B

[Go back to Q214](#)

Explanation to Q214

The scenario is that you can already connect to the EC2 instance via SSH. This means that there is no problem in the Route Table of your VPC. To fix this issue, you simply need to update your Security Group and add an Inbound rule to allow HTTP traffic.

The option that says: In the Security Group, remove the SSH rule is incorrect as doing so will not solve the issue. It will just disable SSH traffic that is already available.

The options that say: In the Route table, add this new route entry: 0.0.0.0 -> igw-b51618cc and In the Route table, add this new route entry: 10.0.0.0/27 -> local are incorrect as there is no need to change the Route Tables.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security_Groups.html

[Go back to Q214](#)

Answer to Q215: D

[Go back to Q215](#)

Explanation to Q215

NA

[Go back to Q215](#)

Answer to Q216: B

[Go back to Q216](#)

Explanation to Q216

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no over-provisioning and paying for additional servers. Fargate runs each task or pod in its own kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design. Therefore, customers such as Vanguard, Accenture, Foursquare, and Ancestry have chosen to run their mission critical applications on Fargate.

Hence, the correct answer is: AWS Fargate.

Amazon EKS is incorrect because this is more suitable to run the Kubernetes management infrastructure and not Docker. It does not remove

the need to provision and manage servers nor let you specify and pay for resources per application, unlike AWS Fargate.

Amazon EFS is incorrect because this is a file system for Linux-based workloads for use with AWS Cloud services and on-premises resources.

Amazon EBS is incorrect because this is primarily used to provide persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.

References:

<https://aws.amazon.com/fargate/>https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ECS_GetStarted_Fargate.html

[Go back to Q216](#)

Answer to Q217: C

[Go back to Q217](#)

Explanation to Q217

NA

[Go back to Q217](#)

Answer to Q218: A

[Go back to Q218](#)

Explanation to Q218

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and

data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

In this scenario, there is a requirement to have a storage service which will be used by a business intelligence application and where the data must be stored in a columnar fashion. Business Intelligence reporting systems is a type of Online Analytical Processing (OLAP) which Redshift is known to support. In addition, Redshift also provides columnar storage unlike the other options. Hence, the correct answer in this scenario is Amazon Redshift.

References:

https://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html

<https://aws.amazon.com/redshift/>

[Go back to Q218](#)

Answer to Q219: D

[Go back to Q219](#)

Explanation to Q219

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront's globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.

FTP is incorrect because the File Transfer Protocol does not guarantee fast throughput and consistent, fast data transfer.

AWS Direct Connect is incorrect because you have users all around the world and not just on your on-premises data center. Direct Connect would be too costly and is not suitable for this purpose.

Using CloudFront Origin Access Identity is incorrect because this is a feature which ensures that only CloudFront can serve S3 content. It does not increase throughput and ensure fast delivery of content to your customers.

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

[Go back to Q219](#)

Answer to Q220: B

[Go back to Q220](#)

Explanation to Q220

Basically, a database service in which you no longer need to worry about database management tasks such as hardware or software provisioning, setup and configuration is called a fully managed database. This means that AWS fully manages all the database management tasks and the underlying host server. The main differentiator here is the keyword "scaling" in the question. In RDS, you still must manually scale up your resources and create Read Replicas to improve scalability while in DynamoDB, this is automatically done.

DynamoDB is the best option to use in this scenario. It is a fully managed non-relational database service you simply create a database table, set your target utilization for Auto Scaling, and let the service handle the rest. You no longer need to worry about database management tasks such as

hardware or software provisioning, setup and configuration, software patching, operating a reliable, distributed database cluster, or partitioning data over multiple instances as you scale. DynamoDB also lets you backup and restore all your tables for data archival, helping you meet your corporate and governmental regulatory requirements.

RDS is incorrect because this is just a "managed" service and not "fully managed". This means that you still must handle the backups and other administrative tasks such as when the automated OS patching will take place.

Amazon ElastiCache is incorrect because although ElastiCache is fully managed, it is not a database service but an In-Memory Data Store.

Redshift is incorrect because although this is fully managed, it is not a database service but a Data Warehouse.

References:

<https://aws.amazon.com/dynamodb/>
<https://aws.amazon.com/products/databases/>

[Go back to Q220](#)

Answer to Q221: B, D

[Go back to Q221](#)

Explanation to Q221

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3:
Use Server-Side Encryption You request Amazon S3 to

encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
Use Server-Side Encryption with Customer-Provided Keys (SSE-C)
Use Client-Side Encryption You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Use Client-Side Encryption with AWS KMS
Managed Customer Master Key (CMK)
Use Client-Side Encryption Using a Client-Side Master Key

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

[Go back to Q221](#)

Answer to Q222: B, E

[Go back to Q222](#)

Explanation to Q222

The correct answers are:- The total volume of data and number of objects you can store are unlimited.- The largest object that can be uploaded in a single PUT is 5 GB.

The option that says: The largest object that can be uploaded in a single PUT is 5 TB is incorrect as the largest object that can be uploaded in a single PUT is 5 GB and not 5 TB. Remember that the upload limit depends on whether you upload an object using a single PUT operation or via Multipart Upload. The largest object that can be uploaded in a single PUT

is 5 GB. Please take note the phrase "... in a single PUT". If you are using the multipart upload API, then the limit is 5 TB.

The option that says: S3 is an object storage service that provides file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage is incorrect because although S3 is indeed an object storage service, it does not provide file system access semantics. EFS provides this feature but not S3.

The option that says: You can only store ZIP or TAR files in S3 is incorrect as you can store virtually any kind of data in any format in S3.

References:

<https://aws.amazon.com/s3/faqs/><https://docs.aws.amazon.com/AmazonS3/latest/dev/UploadingObjects.html>

[Go back to Q222](#)

Answer to Q223: B, C

[Go back to Q223](#)

Explanation to Q223

Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 15 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it.

To make an Expedited, Standard, or Bulk retrieval, set the Tier parameter in the Initiate Job (POST jobs) REST API request to the option you want, or the equivalent in the AWS CLI or AWS SDKs. If you have purchased provisioned

capacity, then all expedited retrievals are automatically served through your provisioned capacity.

Provisioned capacity ensures that your retrieval capacity for expedited retrievals is available when you need it. Each unit of capacity provides that at least three expedited retrievals can be performed every five minutes and provides up to 150 MB/s of retrieval throughput. You should purchase provisioned retrieval capacity if your workload requires highly reliable and predictable access to a subset of your data in minutes. Without provisioned capacity Expedited retrievals are accepted, except for rare situations of unusually high demand. However, if you require access to Expedited retrievals under all circumstances, you must purchase provisioned retrieval capacity.

Retrieving the data using Amazon Glacier Select is incorrect because this is not an archive retrieval option and is primarily used to perform filtering operations using simple Structured Query Language (SQL) statements directly on your data archive in Glacier.

Using Bulk Retrieval to access the financial data is incorrect because bulk retrievals typically complete within 512 hours hence, this does not satisfy the requirement of retrieving the data within 15 minutes. The provisioned capacity option is also not compatible with Bulk retrievals.

Specifying a range, or portion, of the financial data archive to retrieve is incorrect because using ranged archive retrievals is not enough to meet the requirement of retrieving the whole archive in the given timeframe. In addition, it does not provide additional retrieval capacity which is what the provisioned capacity option can offer.

References:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/glacier-select.html>

[Go back to Q223](#)

Answer to Q224: C

[Go back to Q224](#)

Explanation to Q224

All the answers are correct except for the option that says: Standard queues preserve the order of messages. Only FIFO queues can preserve the order of messages and not standard queues.

Reference:

<https://aws.amazon.com/sqs/faqs/> Check out this Amazon SQS

[Go back to Q224](#)

Answer to Q225: D

[Go back to Q225](#)

Explanation to Q225

NA

[Go back to Q225](#)

Answer to Q226: C

[Go back to Q226](#)

Explanation to Q226

SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

You can host multiple TLS secured applications, each with its own TLS certificate, behind a single load balancer. In order to use SNI, all you need to do is bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client. These features are provided at no additional charge.

To meet the requirements in the scenario, you can 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). Hence, the correct answer is the option that says: 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). Using a wildcard certificate to handle multiple sub-domains and different domains is incorrect because a wildcard certificate can only handle multiple sub-domains but not different domains.

Adding a Subject Alternative Name (SAN) for each additional domain to your certificate is incorrect because although using SAN is correct, you will still have to reauthenticate and reprovision your certificate every time you add a new domain. One of the requirements in the scenario is that you should not have to reauthenticate and reprovision your certificate hence, this solution is incorrect.

The option that says: 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 is incorrect because although it is valid to use dedicated IP addresses to meet this requirement, this solution is not

cost-effective. Remember that if you configure CloudFront to serve HTTPS requests using dedicated IP addresses, you incur an additional monthly charge. The charge begins when you associate your SSL/TLS certificate with your CloudFront distribution. You can just simply upload the certificates to the ALB and use SNI to handle multiple domains in a cost-effective manner.

References:

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-sni/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-https-dedicated-ip-or-sni.html#cnames-https-dedicated-ip>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

[Go back to Q226](#)

Answer to Q227: B, D

[Go back to Q227](#)

Explanation to Q227

AWS Lambda automatically monitors functions on your behalf, reporting metrics through Amazon CloudWatch. These metrics include total invocation requests, latency, and error rates. The throttles, Dead Letter Queues errors, and Iterator age for stream-based invocations are also monitored.

You can monitor metrics for Lambda and view logs by using the Lambda console, the CloudWatch console, the AWS CLI, or the CloudWatch API.

ReservedConcurrentExecutions is incorrect because CloudWatch does not monitor Lambda's reserved concurrent executions. You can view it through

the Lambda console or via CLI manually. IteratorSize and ApproximateAgeOfOldestMessage are incorrect because these two are not Lambda metrics.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-access-metrics.html>

<https://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-metrics.html>

[Go back to Q227](#)

Answer to Q228: D

[Go back to Q228](#)

Explanation to Q228

The best option to take is to deploy four EC2 instances in one Availability Zone and four in another availability zone in the same region behind an Amazon Elastic Load Balancer. In this way, if one availability zone goes down, there is still another available zone that can accommodate traffic.

When the first AZ goes down, the second AZ will only have an initial 4 EC2 instances. This will eventually be scaled up to 8 instances since the solution is using Auto Scaling.

The 110% compute capacity for the 4 servers might cause some degradation of the service, but not a total outage since there are still some instances that handle the requests. Depending on your scale-up configuration in your Auto Scaling group, the additional 4 EC2 instances can be launched in a matter of minutes. T3 instances also have a Burstable Performance capability to burst or go beyond the current compute capacity

of the instance to higher performance as required by your workload. So, your 4 servers will be able to manage 110% compute capacity for a short period of time. This is the power of cloud computing versus our on-premises network architecture. It provides elasticity and unparalleled scalability.

Take note that Auto Scaling will launch additional EC2 instances to the remaining Availability Zone/s in the event of an Availability Zone outage in the region. Hence, the correct answer is the option that says: 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.

The option that says: Deploy eight EC2 instances with Auto Scaling in one Availability Zone behind an Amazon Elastic Load Balancer is incorrect because this architecture is not highly available. If that Availability Zone goes down, then your web application will be unreachable.

The options that say: Deploy four EC2 instances with Auto Scaling in one region and four in another region behind an Amazon Elastic Load Balancer and Deploy two EC2 instances with Auto Scaling in four regions behind an Amazon Elastic Load Balancer are incorrect because the ELB is designed to only run in one region and not across multiple regions.

References:

<https://aws.amazon.com/elasticloadbalancing/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

[Go back to Q228](#)

Answer to Q229: A

[Go back to Q229](#)

Explanation to Q229

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications. You store this configuration in the notification subresource that is associated with a bucket. Amazon S3 provides an API for you to manage this subresource.

Amazon S3 event notifications typically deliver events in seconds but can sometimes take a minute or longer. If two writes are made to a single non-versioned object at the same time, it is possible that only a single event notification will be sent. If you want to ensure that an event notification is sent for every successful write, you can enable versioning on your bucket. With versioning, every successful write will create a new version of your object and will also send an event notification.

Amazon S3 can publish notifications for the following events:

1. New object created events
2. Object removal events
3. Restore object events
4. Reduced Redundancy Storage (RRS) object lost events
5. Replication events

Amazon S3 supports the following destinations where it can publish events:

1. Amazon Simple Notification Service (Amazon SNS) topic
2. Amazon Simple Queue Service (Amazon SQS) queue

3. AWS Lambda

If your notification ends up writing to the bucket that triggers the notification, this could cause an execution loop. For example, if the bucket triggers a Lambda function each time an object is uploaded and the function uploads an object to the bucket, then the function indirectly triggers itself. To avoid this, use two buckets, or configure the trigger to only apply to a prefix used for incoming objects.

Hence, the correct answer is: 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.

The option that says: 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 is incorrect because there is no s3:ObjectAdded:* type in Amazon S3. You should add an S3 event notification configuration on the bucket to publish events of the s3:ObjectCreated:* type instead. Moreover, Amazon S3 does not support Amazon MQ as a destination to publish events.

The option that says: 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 is incorrect because the s3:ObjectRemoved:DeleteMarkerCreated type is only triggered when a delete marker is created for a versioned object and not when an object is deleted or a versioned object is permanently deleted.

The option that says: 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 is incorrect because Amazon S3 does not support publishing public event messages to Amazon MQ. You should use an Amazon SQS instead. In

addition, the s3:ObjectRemoved:DeleteMarkerCreated type is only triggered when a delete marker is created for a versioned object. Remember that the scenario asked to publish events when an object is deleted, or a versioned object is permanently deleted.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html>

<https://aws.amazon.com/blogs/aws/s3-event-notification/>

[Go back to Q229](#)

Answer to Q230: D, E

[Go back to Q230](#)

Explanation to Q230

NA

[Go back to Q230](#)

Answer to Q231: B

[Go back to Q231](#)

Explanation to Q231

NA

[Go back to Q231](#)

Answer to Q232: A, D

[Go back to Q232](#)

Explanation to Q232

NA

[Go back to Q232](#)

Answer to Q233: A

[Go back to Q233](#)

Explanation to Q233

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

The Multipart upload API enables you to upload large objects in parts. You can use this API to upload new large objects or make a copy of an existing object. Multipart uploading is a three-step process: you initiate the upload, you upload the object parts, and after you have uploaded all the parts, you complete the multipart upload. Upon receiving the complete multipart upload request, Amazon S3 constructs the object from the uploaded parts and you can then access the object just as you would any other object in your bucket.

Using a single PUT request to upload the large file is incorrect because the largest file size you can upload using a single PUT request is 5 GB. Files larger than this will fail to be uploaded.

Using AWS Snowball is incorrect because this is a migration tool that lets you transfer large amounts of data from your on-premises data center to AWS S3 and vice versa. This tool is not suitable for the given scenario. And when you provision Snowball, the device gets transported to you, and not to your customers. Therefore, you bear the responsibility of securing the device.

Using AWS Import/Export is incorrect because Import/Export is similar to AWS Snowball in such a way that it is meant to be used as a migration tool, and not for multiple customer consumption such as in the given scenario.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>

<https://aws.amazon.com/s3/faqs/>

[Go back to Q233](#)

Answer to Q234: C, D

[Go back to Q234](#)

Explanation to Q234

NA

[Go back to Q234](#)

Answer to Q235: C

[Go back to Q235](#)

Explanation to Q235

There is no additional charge for AWS CloudFormation. You pay for AWS resources (such as Amazon EC2 instances, Elastic Load Balancing load balancers, etc.) created using AWS CloudFormation in the same manner as if you created them manually. You only pay for what you use, as you use it; there are no minimum fees and no required upfront commitments.

The option that says: \$2.50 per template per month is incorrect. There is no cost for creating CloudFormation templates. Costs are calculated from the AWS resources that are provisioned from that CloudFormation template.

The option that says: The length of time it takes to build the architecture with CloudFormation is incorrect. There is no cost for the time it takes to execute CloudFormation templates. Costs are calculated from the AWS resources that are provisioned from that CloudFormation template.

The option that says: It depends on the region where you will deploy is incorrect. Costs per region are not calculated based on the CloudFormation template, but rather on the regions where resources are provisioned during the building of the environment using the CloudFormation template.

Reference:

<https://aws.amazon.com/cloudformation/pricing/>

[Go back to Q235](#)

Answer to Q236: B

[Go back to Q236](#)

[Explanation to Q236](#)

The answer is No. The standby instance will not perform any read and write operations while the primary instance is running.

Multi-AZ deployments for the MySQL, MariaDB, Oracle, and PostgreSQL engines utilize synchronous physical replication to keep data on the standby up-to-date with the primary. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring technology. Both approaches safeguard your data in the event of a DB Instance failure or loss of an Availability Zone.

If a storage volume on your primary instance fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby (or to a replica in the case of Amazon Aurora). Compare this to a Single-AZ deployment: in case of a Single-AZ database failure, a user-initiated point-in-time-restore operation will be required. This operation can take several hours to complete, and any data updates that occurred after the latest restorable time (typically within the last five minutes) will not be available.

The rest of the options are incorrect because regardless of the database engine, you cannot use a standby database for read and write operations.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q236](#)

Answer to Q237: A, D

[Go back to Q237](#)

Explanation to Q237

This question did not mention the specific type of EC2 instance however, it says that it will be stopped and started. Since only EBS-backed instances can be stopped and restarted, it is implied that the instance is EBS-backed. Remember that an instance store-backed instance can only be rebooted or terminated, and its data will be erased if the EC2 instance is either stopped or terminated.

If you stopped an EBS-backed EC2 instance, the volume is preserved but the data in any attached Instance store volumes will be erased. Keep in mind that an EC2 instance has an underlying physical host computer. If the instance is stopped, AWS usually moves the instance to a new host computer. Your instance may stay on the same host computer if there are no problems with the host computer. In addition, its Elastic IP address is disassociated from the instance if it is an EC2-Classic instance. Otherwise, if it is an EC2-VPC instance, the Elastic IP address remains associated.

Take note that an EBS-backed EC2 instance can have attached Instance Store volumes. This is the reason why there is an option that mentions the Instance Store volume, which is placed to test your understanding of this specific storage type. You can launch an EBS-backed EC2 instance and attach several Instance Store volumes but remember that there are some EC2 Instance types that don't support this kind of set up:

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ComponentsAMIs.html#storage-for-the-root-device>

[Go back to Q237](#)

Answer to Q238: A

[Go back to Q238](#)

Explanation to Q238

Amazon Kinesis Data Streams is used to collect and process large streams of data records in real time. You can use Kinesis Data Streams for rapid and continuous data intake and aggregation. The type of data used includes IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real time, the processing is typically lightweight.

The following diagram illustrates the high-level architecture of Kinesis Data Streams. The producers continually push data to Kinesis Data Streams, and the consumers process the data in real time. Consumers (such as a custom application running on Amazon EC2 or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3. Amazon S3 is incorrect because this is mainly used for object storage of frequently and infrequently accessed files with high durability. It does not meet the requirement of being able to collect and process large streams of data in real time. You must use Kinesis data streams instead.

Amazon Redshift is incorrect because this is mainly used for data warehousing making it simple and cost-effective to analyze your data across your data warehouse and data lake. Again, it does not meet the requirement of being able to collect and process large streams of data real time.

Amazon SWF is incorrect because this is mainly used to build applications that use Amazon's cloud to coordinate work across distributed components and not used to process large streams of data records.

Reference:

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

[Go back to Q238](#)

Answer to Q239: B, C

[Go back to Q239](#)

Explanation to Q239

Enabling EBS Encryption and enabling Amazon S3 Server-Side or use Client-Side Encryption are correct. Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.

In Amazon S3, data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options to protect data at rest in Amazon S3. Use Server-Side Encryption. You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption. You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Creating an EBS Snapshot is incorrect because this is a backup solution of EBS. It does not provide security of data inside EBS volumes when executed.

Migrating the EC2 instances from the public to private subnet is incorrect because the data you want to secure are those in EBS volumes and S3 buckets. Moving your EC2 instance to a private subnet involves a different matter of security practice, which does not achieve what you want in this scenario.

Using AWS Shield and WAF is incorrect because these protect you from common security threats for your web applications. However, what you are trying to achieve is securing and encrypting your data inside EBS and S3.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

[Go back to Q239](#)

Answer to Q240: B

[Go back to Q240](#)

Explanation to Q240

The revoke-security-group-ingress command removes one or more ingress rules from a security group.

Each rule consists of the protocol and the CIDR range or source security group. For the TCP and UDP protocols, you must also specify the destination port or range of ports. For the ICMP protocol, you must also specify the ICMP type and code. If the security group rule has a description, you do not have to specify the description to revoke the rule.

Rule changes are propagated to instances within the security group as quickly as possible. However, a small delay might occur. This example removes TCP port 22 access for the 203.0.113.0/24 address range from the security group named MySecurityGroup. If the command succeeds, no output is returned.

Command:`aws ec2 revoke-security-group-ingress --group-name MySecurityGroup --protocol tcp --port 22 --cidr 203.0.113.0/24`

References:

<https://docs.aws.amazon.com/cli/latest/reference/ec2/revoke-security-group-ingress.html>

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

[Go back to Q240](#)

Answer to Q241: A, C

[Go back to Q241](#)

[Explanation to Q241](#)

NA

[Go back to Q241](#)

Answer to Q242: B

[Go back to Q242](#)

[Explanation to Q242](#)

Amazon EC2 Spot instances are spare compute capacity in the AWS cloud available to you at steep discounts compared to On-Demand prices. It can be interrupted by AWS EC2 with two minutes of notification when the EC2 needs the capacity back.

To use Spot Instances, you create a Spot Instance request that includes the number of instances, the instance type, the Availability Zone, and the maximum price that you are willing to pay per instance hour. If your maximum price exceeds the current Spot price, Amazon EC2 fulfills your request immediately if capacity is available. Otherwise, Amazon EC2 waits until your request can be fulfilled or until you cancel the request.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>

<https://aws.amazon.com/ec2/spot/>

[Go back to Q242](#)

Answer to Q243: B

[Go back to Q243](#)

Explanation to Q243

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances.

Reserved Instances are recommended for:- Applications with steady state usage- Applications that may require reserved capacity- Customers that can commit to using EC2 over a 1- or 3-year term to reduce their total computing costs.

References:

<https://aws.amazon.com/ec2/pricing/>
<https://aws.amazon.com/ec2/pricing/reserved-instances/>

[Go back to Q243](#)

Answer to Q244: C

[Go back to Q244](#)

Explanation to Q244

You are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic Spot limit per region. New AWS accounts may start with limits that are lower than the limits described here.

If you need more instances, complete the Amazon EC2 limit increase request form with your use case, and your limit increase will be considered. Limit increases are tied to the region they were requested for.

Hence, the correct answer is: 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.

The option that says: There was an issue with the Amazon EC2 API. Just resend the requests and these will be provisioned successfully is incorrect because you are limited to running On-Demand Instances per your vCPU-based On-Demand Instance limit. There is also a limit of purchasing 20 Reserved Instances and requesting Spot Instances per your dynamic Spot limit per region hence, there is no problem with the EC2 API.

The option that says: By default, AWS allows you to provision a maximum of 20 instances per region. Select a different region and retry the failed request is incorrect. There is no need to select a different region since this limit can be increased after submitting a request form to AWS.

The option that says: 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 is incorrect because the vCPU-based On-Demand Instance limit is set per region and not per Availability Zone. This can be increased after submitting a request form to AWS.

References:

https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2

[Go back to Q244](#)

Answer to Q245: D

[Go back to Q245](#)

Explanation to Q245

A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance.

You can specify your launch configuration with multiple Auto Scaling groups. However, you can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for an Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration.

For this scenario, you must create a new launch configuration. Remember that you can't modify a launch configuration after you've created it.

Hence, the correct answer is: Create a new launch configuration.

The option that says: Do nothing. You can start directly launching EC2 instances in the Auto Scaling group with the same launch configuration is incorrect because what you are trying to achieve is change the AMI being used by your fleet of EC2 instances. Therefore, you need to change the launch configuration to update what your instances are using.

The option that says: create a new target group and create a new target group and launch configuration are both incorrect because you only want to change the AMI being used by your instances, and not the instances themselves. Target groups are primarily used in ELBs and not in Auto Scaling. The scenario didn't mention that the architecture has a load balancer. Therefore, you should be updating your launch configuration, not the target group.

References:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

[Go back to Q245](#)

Answer to Q246: A, C

[Go back to Q246](#)

Explanation to Q246

A VPC spans all the Availability Zones in the region. After creating a VPC, you can add one or more subnets in each Availability Zone. When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. Availability Zones are distinct

locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location.

Below are the important points you have to remember about subnets:-
Each subnet maps to a single Availability Zone.- Every subnet that you create is automatically associated with the main route table for the VPC.- If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet.

The option that says: EC2 instances in a private subnet can communicate with the Internet only if they have an Elastic IP is incorrect because EC2 instances in a private subnet can communicate with the Internet not just by having an Elastic IP, but also with a public IP address via a NAT Instance or a NAT Gateway. Take note that there is a distinction between private and public IP addresses. To enable communication with the Internet, a public IPv4 address is mapped to the primary private IPv4 address through network address translation (NAT).The option that says: The allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /27 netmask (16 IP addresses) is incorrect because the allowed block size in VPC is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses) and not /27 netmask. For you to easily remember this, /27 netmask is equivalent to exactly 27 IP addresses but keep in mind that the limit is until /28 netmask.

The option that says: Each subnet spans to 2 Availability Zones is incorrect because each subnet must reside entirely within one Availability Zone and cannot span zones.

References:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>

[Go back to Q246](#)

Answer to Q247: A

[Go back to Q247](#)

Explanation to Q247

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

Amazon VPC is incorrect because a VPC is a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. It does not provide you the auditing information that were asked for in this scenario.

Amazon EC2 is incorrect because EC2 is a service that provides secure, resizable compute capacity in the cloud and does not provide the needed information in this scenario just like the option above.

Amazon CloudWatch is incorrect because this is a monitoring tool for your AWS resources. Like the above options, it does not provide the needed information to satisfy the requirement in the scenario.

Reference:

<https://aws.amazon.com/cloudtrail/>

[Go back to Q247](#)

Answer to Q248: D, E

[Go back to Q248](#)

Explanation to Q248

You can configure a function to connect to a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud (Amazon VPC) to create a private network for resources such as databases, cache instances, or internal services. Connect your function to the VPC to access private resources during execution.

AWS Lambda runs your function code securely within a VPC by default. However, to enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function to connect securely to other resources within your private VPC.

Lambda functions cannot connect directly to a VPC with dedicated instance tenancy. To connect to resources in a dedicated VPC, peer it to a second VPC with default tenancy.

Your Lambda function automatically scales based on the number of events it processes. If your Lambda function accesses a VPC, you must make sure that your VPC has enough ENI capacity to support the scale requirements of your Lambda function. It is also recommended that you specify at least one subnet in each Availability Zone in your Lambda function configuration.

By specifying subnets in each of the Availability Zones, your Lambda function can run in another Availability Zone if one goes down or runs out of IP addresses. If your VPC does not have enough ENIs or subnet IPs, your Lambda function will not scale as requests increase, and you will see an increase in invocation errors with EC2 error types like EC2ThrottledException. For asynchronous invocation, if you see an increase in errors without corresponding CloudWatch Logs, invoke the Lambda function synchronously in the console to get the error responses.

Hence, the correct answers for this scenario are:- 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.- Your VPC does not have enough subnet ENIs or subnet IPs.

The option that says: Your VPC does not have a NAT gateway is incorrect because an issue in the NAT Gateway is unlikely to cause a request throttling issue or produce an EC2ThrottledException error in Lambda. Take note that the scenario says that the issue is happening only on certain times of the day, which means that the issue is only intermittent, and the function works at other times. We can also conclude that an availability issue is not an issue since the application is already using a highly available NAT Gateway and not just a NAT instance.

The option that says: The associated security group of your function does not allow outbound connections is incorrect because if the associated security group does not allow outbound connections then the Lambda function will not work at all in the first place. Remember that the scenario

says that the issue only happens intermittently. In addition, Internet traffic restrictions do not usually produce EC2ThrottledException errors.

The option that says: The attached IAM execution role of your function does not have the necessary permissions to access the resources of your VPC is incorrect because just as what is explained above, the issue is intermittent and thus, the IAM execution role of the function does have the necessary permissions to access the resources of the VPC since it works at those specific times.

In case that the issue is indeed caused by a permission problem, then an EC2AccessDeniedException the error would most likely be returned and not an EC2ThrottledException error.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/vpc.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/>

<https://aws.amazon.com/premiumsupport/knowledge-center/lambda-troubleshoot-invoke-error-502-500/>

[Go back to Q248](#)

Answer to Q249: C

[Go back to Q249](#)

Explanation to Q249

S3 Select enables applications to retrieve only a subset of data from an object by using simple SQL expressions. By using S3 Select to retrieve only

the data needed by your application, you can achieve drastic performance increases.

Amazon S3 is composed of buckets, object keys, object metadata, object tags, and many other components as listed below:

1. An Amazon S3 bucket name is globally unique, and the namespace is shared by all AWS accounts.
2. An Amazon S3 object key refers to the key name, which uniquely identifies the object in the bucket.
3. An Amazon S3 object metadata is a name-value pair that provides information about the object.
4. An Amazon S3 object tag is a key-pair value used for object tagging to categorize storage.

You can perform S3 Select to query only the necessary data inside the CSV files based on the bucket's name and the object's key.

The following snippet below shows how it is done using boto3 (AWS SDK for Python):

```
client = boto3.client('s3') resp = client.select_object_content(  
Bucket='tdojo-bucket', # Bucket Name. Key='s3-select/techradiofile.csv', #  
Object Key. ExpressionType= 'SQL', Expression = "select \"Sample\" from  
s3object s where s.\"techradiofile\" in ['A', 'B']"
```

Hence, the correct answer is the option that says: Perform an S3 Select operation based on the bucket's name and object's key.

The option that says: Perform an S3 Select operation based on the bucket's name and object's metadata is incorrect because metadata is not needed when querying subsets of data in an object using S3 Select.

The option that says: Perform an S3 Select operation based on the bucket's name and object tags is incorrect because object tags just provide additional information to your object. This is not needed when querying with S3 Select although this can be useful for S3 Batch Operations. You can categorize objects based on tag values to provide S3 Batch Operations with a list of objects to operate on.

The option that says: Perform an S3 Select operation based on the bucket's name is incorrect because you need both the buckets name and the object key to successfully perform an S3 Select operation.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-glacier-select-sql-reference-select.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingObjects.html>

[Go back to Q249](#)

Answer to Q250: A

[Go back to Q250](#)

Explanation to Q250

Kinesis Data Streams supports changes to the data record retention period of your stream. A Kinesis data stream is an ordered sequence of data records meant to be written to and read from in real-time. Data records are therefore stored in shards in your stream temporarily.

The time period from when a record is added to when it is no longer accessible is called the retention period. A Kinesis data stream stores records from 24 hours by default to a maximum of 168 hours.

This is the reason why there are missing data in your S3 bucket. To fix this, you can either configure your sensors to send the data everyday instead of every other day or alternatively, you can increase the retention period of your Kinesis data stream.

The option that says: There is a problem in the sensors. They probably had some intermittent connection hence; the data is not sent to the stream is incorrect. You already verified that the sensors are working as they should be hence, this is not the root cause of the issue.

The option that says: By default, Amazon S3 stores the data for 1 day and moves it to Amazon Glacier is incorrect because by default, Amazon S3 does not store the data for 1 day and moves it to Amazon Glacier.

The option that says: Your AWS account was hacked and someone has deleted some data in your Kinesis stream is incorrect because although this could be a possibility, you should verify first if there are other more probable reasons for the missing data in your S3 bucket. Be sure to follow and apply security best practices as well to prevent being hacked by someone. By default, the data records are only accessible for 24 hours from the time they are added to a Kinesis stream, which depicts the root cause of this issue.

Reference:

<http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>

[Go back to Q250](#)

Answer to Q251: B, D

[Go back to Q251](#)

Explanation to Q251

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3.

Use Server-Side Encryption You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

Use Client-Side Encryption You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Hence, the following options are the correct answers:-

- Enable SSE on an S3 bucket to make use of AES-256 encryption-
- Encrypt the data using your own encryption keys then copy the data to Amazon S3 over HTTPS endpoints. This refers to using a Server-Side Encryption with Customer-Provided Keys (SSE-C).
- Storing the data in encrypted EBS snapshots and storing the data on EBS volumes with encryption enabled instead of using Amazon S3 are both incorrect because all these options are for protecting your data in your EBS volumes. Note that an S3 bucket does not use EBS volumes to store your data.

Using AWS Shield to protect your data at rest is incorrect because AWS Shield is mainly used to protect your entire VPC against DDoS attacks.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

[Go back to Q251](#)

Answer to Q252: D

[Go back to Q252](#)

Explanation to Q252

ElastiCache improves the performance of your database through caching query results.

The primary purpose of an in-memory key-value store is to provide ultra-fast (sub millisecond latency) and inexpensive access to copies of data. Most data stores have areas of data that are frequently accessed but seldom updated. Additionally, querying a database is always slower and more expensive than locating a key in a key-value pair cache. Some database queries are especially expensive to perform, for example, queries that involve joins across multiple tables or queries with intensive calculations.

By caching such query results, you pay the price of the query once and then can quickly retrieve the data multiple times without having to re-execute the query.

The option that says: It securely delivers data to customers globally with low latency and high transfer speeds is incorrect because this option describes what CloudFront does and not ElastiCache.

The option that says: 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 is incorrect because this option describes what Amazon DynamoDB Accelerator (DAX) does and not ElastiCache. Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB. Amazon ElastiCache cannot provide a performance improvement from milliseconds to microseconds, let alone millions of requests per second like DAX can.

The option that says: It reduces the load on your database by routing read queries from your applications to the Read Replica is incorrect because this option describes what an RDS Read Replica does and not ElastiCache.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region.

References:

<https://aws.amazon.com/elasticache/>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-use-cases.html>

[Go back to Q252](#)

Answer to Q253: C

[Go back to Q253](#)

Explanation to Q253

When the word durability pops out, the first service that should come to your mind is Amazon S3. Since this service is not available in the answer options, we can look at the other data store available which is Amazon DynamoDB.

DynamoDB is durable, scalable, and highly available data store which can be used for real-time tabulation. You can also use AppSync with DynamoDB to make it easy for you to build collaborative apps that keep shared data updated in real time. You just specify the data for your app with simple code statements and AWS AppSync manages everything needed to keep the app data updated in real time. This will allow your app to access data in Amazon DynamoDB, trigger AWS Lambda functions, or run Amazon Elasticsearch queries and combine data from these services to provide the exact data you need for your app.

Amazon Redshift and AWS Mobile Hub are incorrect as Amazon Redshift is mainly used as a data warehouse and for online analytic processing (OLAP). Although this service can be used for this scenario, DynamoDB is still the top choice given its better durability and scalability.

Amazon Relational Database Service (RDS) and Amazon MQ and Amazon Aurora and Amazon Cognito are possible answers in this scenario, however, DynamoDB is much more suitable for simple mobile apps which do not have complicated data relationships compared with enterprise web applications. The scenario says that the mobile app will be used from around the world, which is why you need a data storage service which can be supported globally. It would be a management overhead to implement multi-region deployment for your RDS and Aurora database instances compared to using the Global table feature of DynamoDB.

References:

<https://aws.amazon.com/dynamodb/faqs/>

<https://aws.amazon.com/appsync/>

[Go back to Q253](#)

Answer to Q254: A

[Go back to Q254](#)

Explanation to Q254

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload.

Depending on the type of workload, you can create a placement group using one of the following placement strategies.

Cluster packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Partition spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

Spread strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when most of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.

Partition placement groups can be used to deploy large distributed and replicated workloads, such as HDFS, HBase, and Cassandra, across distinct racks. When you launch instances into a partition placement group, Amazon EC2 tries to distribute the instances evenly across the number of partitions that you specify. You can also launch instances into a specific partition to have more control over where the instances are placed.

Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other. Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same racks. Spread placement groups provide access to distinct racks and are therefore suitable for mixing instance types or launching instances over

time. A spread placement group can span multiple Availability Zones in the same Region. You can have a maximum of seven running instances per Availability Zone per group.

Hence, the correct answer is: Set up a cluster placement group within a single Availability Zone in the same AWS Region.

The option that says: Set up a spread placement group across multiple Availability Zones in multiple AWS Regions is incorrect because although using a placement group is valid for this particular scenario, you can only set up a placement group in a single AWS Region only. A spread placement group can span multiple Availability Zones in the same Region.

The option that says: Set up AWS Direct Connect connections across multiple Availability Zones for increased bandwidth throughput and more consistent network experience is incorrect because this is primarily used for hybrid architectures. It bypasses the public Internet and establishes a secure, dedicated connection from your on-premises data center into AWS, and not used for having low latency within your AWS network.

The option that says: Use EC2 Dedicated Instances is incorrect because these are EC2 instances that run in a VPC on hardware that is dedicated to a single customer and are physically isolated at the host hardware level from instances that belong to other AWS accounts. It is not used for reducing latency.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

<https://aws.amazon.com/hpc/>

[Go back to Q254](#)

Answer to Q255: D

[Go back to Q255](#)

Explanation to Q255

Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone and improves your application's ability to handle the loss of one or more instances.

When you create a Classic Load Balancer, the default for cross-zone load balancing depends on how you create the load balancer. With the API or CLI, cross-zone load balancing is disabled by default. With the AWS Management Console, the option to enable cross-zone load balancing is selected by default. After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time.

The following diagrams demonstrate the effect of cross-zone load balancing. There are two enabled Availability Zones, with 2 targets in Availability Zone A and 8 targets in Availability Zone B. Clients send requests, and Amazon Route 53 responds to each request with the IP address of one of the load balancer nodes. This distributes traffic such that each load balancer node receives 50% of the traffic from the clients. Each load balancer node distributes its share of the traffic across the registered targets in its scope.

If cross-zone load balancing is enabled, each of the 10 targets receives 10% of the traffic. This is because each load balancer node can route its 50% of the client traffic to all 10 targets.

If cross-zone load balancing is disabled, each of the 2 targets in Availability Zone A receives 25% of the traffic and each of the 8 targets in Availability Zone B receives 6.25% of the traffic. This is because each load balancer node can route its 50% of the client traffic only to targets in its Availability Zone.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html#cross-zone-load-balancing>

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html>

[Go back to Q255](#)

Answer to Q256: B

[Go back to Q256](#)

Explanation to Q256

Amazon Aurora typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When you connect to an Aurora cluster, the hostname and port that you specify point to an intermediate handler called an endpoint. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren't available.

For certain Aurora tasks, different instances or groups of instances perform different roles. For example, the primary instance handles all data definition language (DDL) and data manipulation language (DML) statements. Up to 15 Aurora Replicas handle read-only query traffic.

Using endpoints, you can map each connection to the appropriate instance or group of instances based on your use case. For example, to perform DDL statements you can connect to whichever instance is the primary instance. To perform queries, you can connect to the reader endpoint, with Aurora automatically performing load-balancing among all the Aurora Replicas. For clusters with DB instances of different capacities or configurations, you can connect to custom endpoints associated with different subsets of DB

instances. For diagnosis or tuning, you can connect to a specific instance endpoint to examine details about a specific DB instance.

A reader endpoint for an Aurora DB cluster provides load-balancing support for read-only connections to the DB cluster. Use the reader endpoint for read operations, such as queries. By processing those statements on the read-only Aurora Replicas, this endpoint reduces the overhead on the primary instance. It also helps the cluster to scale the capacity to handle simultaneous SELECT queries, proportional to the number of Aurora Replicas in the cluster. Each Aurora DB cluster has one reader endpoint.

If the cluster contains one or more Aurora Replicas, the reader endpoint load-balances each connection request among the Aurora Replicas. In that case, you can only perform read-only statements such as SELECT in that session. If the cluster only contains a primary instance and no Aurora Replicas, the reader endpoint connects to the primary instance. In that case, you can perform write operations through the endpoint.

Hence, the correct answer is to use the built-in Reader endpoint of the Amazon Aurora database.

The option that says: Use the built-in Cluster endpoint of the Amazon Aurora database is incorrect because a cluster endpoint (also known as a writer endpoint) simply connects to the current primary DB instance for that DB cluster. This endpoint can perform write operations in the database such as DDL statements, which is perfect for handling production traffic but not suitable for handling queries for reporting since there will be no write database operations that will be sent.

The option that says: Enable Amazon Aurora Parallel Query is incorrect because this feature simply enables Amazon Aurora to push down and distribute the computational load of a single query across thousands of CPUs in Aurora's storage layer. Take note that it does not load balance all the incoming read requests equally to the two Read Replicas. With Parallel Query, query processing is pushed down to the Aurora storage layer. The

query gains a large amount of computing power, and it needs to transfer far less data over the network. In the meantime, the Aurora database instance can continue serving transactions with much less interruption. This way, you can run transactional and analytical workloads alongside each other in the same Aurora database, while maintaining high performance.

The option that says: Create a new Network Load Balancer to evenly distribute the read queries to the Read Replicas of the Amazon Aurora database is incorrect because a Network Load Balancer is not the suitable service/component to use for this requirement since an NLB is primarily used to distribute traffic to servers, not Read Replicas. You must use the built-in Reader endpoint of the Amazon Aurora database instead.

References:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html>

<https://aws.amazon.com/rds/aurora/parallel-query/>

[Go back to Q256](#)

Answer to Q257: C, D

[Go back to Q257](#)

Explanation to Q257

You can use a combination of EC2 and SWF for the following scenarios:

1. Managing a multi-step and multi-decision checkout process of an e-commerce mobile app. Orchestrating the execution of distributed business processes.
2. Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. Amazon SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks. Tasks represent invocations of various processing steps in an application which can be performed by executable code, web service calls, human actions, and scripts.

The option that says: For a distributed session management for your mobile application is incorrect as ElastiCache is the best option for distributed session management.

The option that says: For applications that require a message queue is incorrect as SQS is the best service to use as a message queue.

The option that says: For web applications that require content delivery networks is incorrect as CloudFront is the best option for applications that require a global content delivery network.

References:

<https://aws.amazon.com/swf/> <https://aws.amazon.com/ec2/>

[Go back to Q257](#)

Answer to Q258: D

[Go back to Q258](#)

[Explanation to Q258](#)

You can associate the `CreationPolicy` attribute with a resource to prevent its status from reaching `create complete` until AWS CloudFormation receives a specified number of success signals or the timeout period is exceeded. To signal a resource, you can use the `cfn-signal` helper script or `SignalResource` API. AWS CloudFormation publishes valid signals to the stack events so that you track the number of signals sent.

The creation policy is invoked only when AWS CloudFormation creates the associated resource. Currently, the only AWS CloudFormation resources that support creation policies are `AWS::AutoScaling::AutoScalingGroup`, `AWS::EC2::Instance`, and `AWS::CloudFormation::WaitCondition`.

Use the `CreationPolicy` attribute when you want to wait on resource configuration actions before stack creation proceeds. For example, if you install and configure software applications on an EC2 instance, you might want those applications to be running before proceeding. In such cases, you can add a `CreationPolicy` attribute to the instance, and then send a success signal to the instance after the applications are installed and configured.

Hence, the option that says: 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 is correct.

The option that says: 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 is incorrect because the `cfn-init` helper script is not suitable to be used to signal another resource. You must use `cfn-signal` instead. And although you can use the `DependsOn` attribute to ensure the creation of a specific resource follows another, it is still better to use the `CreationPolicy` attribute instead as it ensures that the applications are properly running before the stack creation proceeds.

The option that says: 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 is incorrect because the `UpdatePolicy` attribute is primarily used for updating resources and for stack update rollback operations.

The option that says: 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 is incorrect because the `UpdateReplacePolicy` attribute is primarily used to retain or in some cases, back up the existing physical instance of a resource when it is replaced during a stack update operation.

References:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-creationpolicy.html>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying-applications.html#deployment-walkthrough-cfn-signal>

<https://aws.amazon.com/blogs/devops/use-a-creationpolicy-to-wait-for-on-instance-configurations/>

[Go back to Q258](#)

Answer to Q259: D

[Go back to Q259](#)

Explanation to Q259

In this scenario, it is best to use a combination of Amazon S3 and Amazon EMR: Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files. Access logging in the ELB is stored in Amazon S3 which means

that the following are valid options:- Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application.- Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files.

However, log analysis can be automatically provided by Amazon EMR, which is more economical than building a custom-built log analysis application and hosting it in EC2. Hence, the option that says: Amazon S3 for storing ELB log files and Amazon EMR for analyzing the log files is the best answer between the two.

Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logging at any time.

Amazon EMR provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. It securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics. You can also run other popular distributed frameworks such as Apache Spark, HBase, Presto, and Flink in Amazon EMR, and interact with data in other AWS data stores such as Amazon S3 and Amazon DynamoDB.

The option that says: Amazon DynamoDB for storing and EC2 for analyzing the logs is incorrect because DynamoDB is a NoSQL database solution of AWS. It would be inefficient to store logs in DynamoDB while using EC2 to analyze them.

The option that says: Amazon EC2 with EBS volumes for storing and analyzing the log files is incorrect because using EC2 with EBS would be costly, and EBS might not provide the most durable storage for your logs, unlike S3.

The option that says: Amazon S3 for storing the ELB log files and an EC2 instance for analyzing the log files using a custom-built application is incorrect because using EC2 to analyze logs would be inefficient and expensive since you will have to program the analyzer yourself.

References:

<https://aws.amazon.com/emr/>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

[Go back to Q259](#)

Answer to Q260: D

[Go back to Q260](#)

Explanation to Q260

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

When setting up a bastion host in AWS, you should only allow the individual IP of the client and not the entire network. Therefore, in the Source, the proper CIDR notation should be used. The /32 denotes one IP address and the /0 refers to the entire network.

The option that says: Security Group Inbound Rule: Protocol UDP, Port Range 22, Source 175.45.116.100/32 is incorrect since the SSH protocol uses TCP and port 22, and not UDP.

The option that says: Network ACL Inbound Rule: Protocol UDP, Port Range 22, Source 175.45.116.100/32 is incorrect since the SSH protocol uses TCP and port 22, and not UDP. Aside from that, network ACLs act as a firewall for your whole VPC subnet, while security groups operate on an instance level. Since you are securing an EC2 instance, you should be using security groups.

The option that says: Network ACL Inbound Rule: Protocol TCP, Port Range-22, Source 175.45.116.100/0 is incorrect as it allowed the entire network instead of a single IP to gain access to the host.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

[Go back to Q260](#)

Answer to Q261: B

[Go back to Q261](#)

Explanation to Q261

AWS Lambda supports synchronous and asynchronous invocation of a Lambda function. You can control the invocation type only when you invoke a Lambda function. When you use an AWS service as a trigger, the invocation type is predetermined for each service. You have no control over the invocation type that these event sources use when they invoke your Lambda function. Since the processing only takes 5 minutes, Lambda is also a cost-effective choice.

Using a combination of Lambda and Step Functions to orchestrate service components and asynchronously process the requests is incorrect because the AWS Step Functions service lets you coordinate multiple AWS services

into serverless workflows so you can build and update apps quickly. Although this can be a valid solution, it is not cost-effective since the application does not have a lot of components to orchestrate. Lambda functions can effectively meet the requirements in this scenario without using Step Functions. This service is not as cost-effective as Lambda.

Using a combination of SQS to queue the requests and then asynchronously processing them using On-Demand EC2 Instances and Using a combination of SNS to buffer the requests and then asynchronously processing them using On-Demand EC2 Instances are both incorrect as using On-Demand EC2 instances is not cost-effective. It is better to use a Lambda function instead.

References:

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-invocation.html>

[Go back to Q261](#)

Answer to Q262: B

[Go back to Q262](#)

Explanation to Q262

In this scenario, it is stated that the SQS queue is configured with the maximum message retention period. The maximum message retention in SQS is 14 days that is why the option that says: Tell the users that the application will be operational shortly and all received requests will be processed after the web application is restarted is the correct answer i.e. there will be no missing messages.

The options that say: Tell the users that unfortunately, they have to resubmit all the requests again and Tell the users that the application will be operational shortly, however, requests sent over three days ago will need to be resubmitted are incorrect as there are no missing messages in the queue thus, there is no need to resubmit any previous requests.

The option that says: 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 is incorrect as the queue can contain an unlimited number of messages, not just 10,000 messages.

In Amazon SQS, you can configure the message retention period to a value from 1 minute to 14 days. The default is 4 days. Once the message retention limit is reached, your messages are automatically deleted.

A single Amazon SQS message queue can contain an unlimited number of messages. However, there is a 120,000 limit for the number of inflight messages for a standard queue and 20,000 for a FIFO queue. Messages are inflight after they have been received from the queue by a consuming component but have not yet been deleted from the queue.

Reference:

<https://aws.amazon.com/sqs/>

[Go back to Q262](#)

Answer to Q263: B, E

[Go back to Q263](#)

Explanation to Q263

Here are the prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:- An S3 bucket that is configured to host a static

website. The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain portal.techrad.io, the name of the bucket must be portal.techrad.io.- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

The option that says: The record set must be of type "MX" is incorrect since an MX record specifies the mail server responsible for accepting email messages on behalf of a domain name. This is not what is being asked by the question.

The option that says: The S3 bucket must be in the same region as the hosted zone is incorrect. There is no constraint that the S3 bucket must be in the same region as the hosted zone, for the Route 53 service to route traffic into it.

The option that says: The Cross-Origin Resource Sharing (CORS) option should be enabled in the S3 bucket is incorrect because you only need to enable Cross-Origin Resource Sharing (CORS) when your client web application on one domain interacts with the resources in a different domain.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html>

[Go back to Q263](#)

Answer to Q264: C

[Go back to Q264](#)

Explanation to Q264

AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

Each Snowball Edge device can transport data at speeds faster than the internet. This transport is done by shipping the data in the appliances through a regional carrier. The appliances are rugged shipping containers, complete with E Ink shipping labels. The AWS Snowball Edge device differs from the standard Snowball because it can bring the power of the AWS Cloud to your on-premises location, with local storage and compute functionality.

Snowball Edge devices have three options for device configurations storage optimized, compute optimized, and with GPU.

Hence, the correct answer is: AWS Snowball Edge.

AWS Snowmobile is incorrect because this is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. It is not suitable for transferring a small amount of data, like 80 TB in this scenario. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. A more cost-effective solution here is to order a Snowball Edge device instead.

AWS Direct Connect is incorrect because it is primarily used to establish a dedicated network connection from your premises network to AWS. This is not suitable for one-time data transfer tasks, like what is depicted in the scenario.

Amazon S3 Multipart Upload is incorrect because this feature simply enables you to upload large objects in multiple parts. It still uses the same Internet connection of the company, which means that the transfer will still take time due to its current bandwidth allocation.

References:

<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>

<https://docs.aws.amazon.com/snowball/latest/ug/device-differences.html>

[Go back to Q264](#)

Answer to Q265: C

[Go back to Q265](#)

Explanation to Q265

NA

[Go back to Q265](#)

Answer to Q266: D

[Go back to Q266](#)

Explanation to Q266

Cold HDD volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than Throughput Optimized HDD, this is a good fit ideal for large, sequential cold-data workloads. If you require infrequent access to your data and are looking to save costs, Cold HDD provides inexpensive block storage. Take note that bootable Cold HDD volumes are not supported.

Cold HDD provides the lowest cost HDD volume and is designed for less frequently accessed workloads. Hence, Cold HDD (sc1) is the correct answer.

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has small, random I/O operations or large, sequential I/O operations.

EBS General Purpose SSD (gp2) is incorrect because a General purpose SSD volume costs more and it is mainly used for a wide variety of workloads. It is recommended to be used as system boot volumes, virtual desktops, low-latency interactive apps, and many more.

Provisioned IOPS SSD (io1) is incorrect because this costs more than Cold HDD and thus, not cost-effective for this scenario. It provides the highest performance SSD volume for mission-critical low-latency or high-throughput workloads, which is not needed in the scenario.

Throughput Optimized HDD (st1) is incorrect because this is primarily used for frequently accessed, throughput-intensive workloads. In this scenario, Cold HDD perfectly fits the requirement as it is used for their infrequently accessed data and provides the lowest cost, unlike Throughput Optimized HDD.

References:

<https://aws.amazon.com/ebs/details/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

[Go back to Q266](#)

Answer to Q267: D, E

[Go back to Q267](#)

[Explanation to Q267](#)

In Auto Scaling, the following statements are correct regarding the cooldown period:

1. It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity takes effect.
2. Its default value is 300 seconds.
3. It is a configurable setting for your Auto Scaling group.

The following options are incorrect:

- It ensures that before the Auto Scaling group scales out, the EC2 instances have an ample time to cooldown.
- It ensures that the Auto Scaling group launches or terminates additional EC2 instances without any downtime.
- Its default value is 600 seconds.

These statements are inaccurate and don't depict what the word "cooldown" means for Auto Scaling. The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities.

The figure below demonstrates the scaling cooldown:

Reference:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html>

[Go back to Q267](#)

Answer to Q268: B, E

[Go back to Q268](#)

Explanation to Q268

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a front door for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application. Since it can use AWS Lambda, you can run your APIs without servers.

Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive, and the amount of data transferred out.

Hence, the correct answers are:- Enables you to build RESTful APIs and WebSocket APIs that are optimized for serverless workloads- You pay only for the API calls you receive, and the amount of data transferred out.

The option that says: It automatically provides a query language for your APIs like GraphQL is incorrect because this is not provided by API Gateway.

The option that says: Provides you with static anycast IP addresses that serve as a fixed entry point to your applications hosted in one or more AWS Regions is incorrect because this is a capability of AWS Global Accelerator and not API Gateway.

The option that says: 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 is incorrect because this is a capability of Elastic Fabric Adapter and not API Gateway.

References:

<https://aws.amazon.com/api-gateway/>

<https://aws.amazon.com/api-gateway/features/>

[Go back to Q268](#)

Answer to Q269: A, D

[Go back to Q269](#)

Explanation to Q269

Amazon S3 Standard - Infrequent Access (Standard - IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Standard - IA offers the high durability, throughput, and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

This combination of low cost and high performance make Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

Key Features:- Same low latency and high throughput performance of Standard- Designed for durability of 99.99999999% of objects- Designed for 99.9% availability over a given year- Backed with the Amazon S3 Service

Level Agreement for availability- Supports SSL encryption of data in transit and at rest- Lifecycle management for automatic migration of objects.

The option that says: It is the best storage option to store noncritical and reproducible data is incorrect as it refers to Amazon S3 - Reduced Redundancy Storage (RRS). In addition, RRS will be completely deprecated soon and AWS recommends using S3 IA One-Zone instead.

The option that says: It provides high latency and low throughput performance is incorrect as it should be "low latency" and "high throughput" instead. S3 automatically scales performance to meet user demands.

The option that says: Ideal to use for data archiving is incorrect because this statement refers to Amazon S3 Glacier. Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

[Go back to Q269](#)

Answer to Q270: D

[Go back to Q270](#)

Explanation to Q270

For this scenario, using Route 53 with the failover option to a static S3 website bucket or CloudFront distribution is correct. You can create a new Route 53 with the failover option to a static S3 website bucket or CloudFront distribution as an alternative.

Duplicating the exact application architecture in another region and configuring DNS weight-based routing is incorrect because running a duplicate system is not a cost-effective solution. Remember that you are trying to build a failover mechanism for your web app, not a distributed setup.

Enabling failover to an application hosted in an on-premises data center is incorrect because, although you can set up failover to your on-premises data center, you are not maximizing the AWS environment such as using Route 53 failover.

Adding more servers in case the application fails is incorrect because this is not the best way to handle a failover event. If you add more servers only in case the application fails, then there would be a period of downtime in which your application is unavailable. Since there are no running servers on that period, your application will be unavailable for a certain period until your new server is up and running.

Reference :

<https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

[Go back to Q270](#)

Answer to Q271: D

[Go back to Q271](#)

Explanation to Q271

By default, instances that you launch into a virtual private cloud (VPC) can't communicate with your own network. You can enable access to your network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

Although the term VPN connection is a general term, in the Amazon VPC documentation, a VPN connection refers to the connection between your VPC and your own network. AWS supports Internet Protocol security (IPsec) VPN connections.

A customer gateway is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. Next, you must set up an Internet-routable IP address (static) of the customer gateway's external interface.

The following diagram illustrates single VPN connections. The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.

A dedicated NAT instance in a public subnet and the main route table in your VPC to route traffic through a NAT instance are incorrect since you don't need a NAT instance for you to be able to create a VPN connection.

An EIP to the Virtual Private Gateway is incorrect since you do not attach an EIP to a VPG.

References:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

<https://docs.aws.amazon.com/vpc/latest/userguide/SetUpVPNConnection.html>

[Go back to Q271](#)

Answer to Q272: B

[Go back to Q272](#)

Explanation to Q272

NA

[Go back to Q272](#)

Answer to Q273: A

[Go back to Q273](#)

Explanation to Q273

IP addresses enable resources in your VPC to communicate with each other, and with resources over the Internet. Amazon EC2 and Amazon VPC support the IPv4 and IPv6 addressing protocols.

By default, Amazon EC2 and Amazon VPC use the IPv4 addressing protocol. When you create a VPC, you must assign it an IPv4 CIDR block (a range of private IPv4 addresses). Private IPv4 addresses are not reachable over the Internet. To connect to your instance over the Internet, or to enable communication between your instances and other AWS services that have public endpoints, you can assign a globally-unique public IPv4 address to your instance.

You can optionally associate an IPv6 CIDR block with your VPC and subnets and assign IPv6 addresses from that block to the resources in your VPC.

IPv6 addresses are public and reachable over the Internet.

All subnets have a modifiable attribute that determines whether a network interface created in that subnet is assigned a public IPv4 address and, if applicable, an IPv6 address. This includes the primary network interface (eth0) that's created for an instance when you launch an instance in that subnet. Regardless of the subnet attribute, you can still override this setting for a specific instance during launch.

By default, nondefault subnets have the IPv4 public addressing attribute set to false, and default subnets have this attribute set to true. An exception is a nondefault subnet created by the Amazon EC2 launch instance wizard—the wizard sets the attribute to true. You can modify this attribute using the Amazon VPC console.

In this scenario, there are 5 EC2 instances that belong to the same security group that should be able to connect to the Internet. The main route table is properly configured but there is a problem connecting to one instance. Since the other four instances are working fine, we can assume that the security group and the route table are correctly configured. One possible reason for this issue is that the problematic instance does not have a public or an EIP address.

Take note as well that the four EC2 instances all belong to a public non-default subnet. Which means that a new EC2 instance will not have a public IP address by default since the IPv4 public addressing attribute is initially set to false.

Hence, the correct answer is the option that says: The EC2 instance does not have a public IP address associated with it.

The option that says: The route table is not properly configured to allow traffic to and from the Internet through the Internet gateway is incorrect because the other three instances, which are associated with the same route table and security group, do not have any issues.

The option that says: The EC2 instance is running in an Availability Zone that is not connected to an Internet gateway is incorrect because there is no relationship between the Availability Zone and the Internet Gateway (IGW) that may have caused the issue.

References:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario_1.html

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html#vpc-ip-addressing-subnet>

[Go back to Q273](#)

Answer to Q274: D

[Go back to Q274](#)

Explanation to Q274

AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet.

Snowball is a strong choice for data transfer if you need to more securely and quickly transfer terabytes to many petabytes of data to AWS. Snowball can also be the right choice if you don't want to make expensive upgrades to your network infrastructure, if you frequently experience large backlogs of data, if you're located in a physically isolated environment, or if you're in an area where high-speed Internet connections are not available or cost-prohibitive.

As a rule of thumb, if it takes more than one week to upload your data to AWS using the spare capacity of your existing Internet connection, then you should consider using Snowball. For example, if you have a 100 Mb connection that you can solely dedicate to transferring your data and need to transfer 100 TB of data, it takes more than 100 days to complete data transfer over that connection. You can make the same transfer by using multiple Snowballs in about a week.

Hence, ordering multiple AWS Snowball devices to upload the files to Amazon S3 is the correct answer.

Uploading it directly to S3 is incorrect since this would take too long to finish due to the slow Internet connection of the company.

Establishing an AWS Direct Connect connection then transferring the data over to S3 is incorrect since provisioning a line for Direct Connect would take too much time and might not give you the fastest data transfer solution. In addition, the scenario didn't warrant an establishment of a dedicated connection from your on-premises data center to AWS. The primary goal is to just do a one-time migration of data to AWS which can be accomplished by using AWS Snowball devices.

Using AWS Snowmobile to transfer the data over to S3 is incorrect because Snowmobile is more suitable if you need to move extremely large amounts of data to AWS or need to transfer up to 100PB of data. This will be transported on a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Take note that you only need to migrate 250 TB of data, hence, this is not the most suitable and cost-effective solution.

References:

<https://aws.amazon.com/snowball/>

<https://aws.amazon.com/snowball/faqs/>

[Go back to Q274](#)

Answer to Q275: C

[Go back to Q275](#)

Explanation to Q275

The route table entries enable EC2 instances in the subnet to use IPv4 to communicate with other instances in the VPC, and to communicate directly over the Internet. A subnet that's associated with a route table that has a route to an Internet gateway is known as a public subnet.

If you could not connect to your EC2 instance even if there is already an Internet Gateway in your VPC and there is no issue in the security group, then you must check if the entries in the route table are properly configured.

Setting an Elastic IP Address to the EC2 instance is incorrect since you already have a public IP address for your EC2 instance and doesn't require an EIP anymore.

Setting a Secondary Private IP Address to the EC2 instance is incorrect because having a secondary private IP address is only used within the VPC, not when connecting to the outside Internet.

Checking the CloudWatch logs as there must be some issue in the EC2 instance is incorrect because it is better to go through your setup and make sure that you didn't miss a step, such as adding a route in the route table, before you check the actual CloudWatch logs to see if an instance has an issue.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario_1.html

[Go back to Q275](#)

Answer to Q276: C

[Go back to Q276](#)

Explanation to Q276

One of the best practices in Amazon IAM is to grant least privilege.

When you create IAM policies, follow the standard security advice of granting least privilege, that is, granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Therefore, using the principle of least privilege which means granting only the permissions required to perform a task is the correct answer.

Start with a minimum set of permissions and grant additional permissions as necessary.

Defining the right set of permissions requires some understanding of the user's objectives. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.

Granting all permissions to any EC2 user is incorrect since you don't want your users to gain access to everything and perform unnecessary actions. Doing so is not a good security practice.

Using the principle of least privilege which means granting only the least number of people with full root access is incorrect because this is not the correct definition of what the principle of least privilege is.

Determining what users need to do and then craft policies for them that let the users perform those tasks including additional administrative operations is incorrect as well since there are some users who you should not give administrative access to. You should follow the principle of least privilege when providing permissions and accesses to your resources.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions>

[Go back to Q276](#)

Answer to Q277: C, E

[Go back to Q277](#)

Explanation to Q277

Amazon Simple Queue Service (SQS) and Amazon Simple Workflow Service (SWF) are the services that you can use for creating a decoupled architecture in AWS. Decoupled architecture is a type of computing architecture that enables computing components or layers to execute independently while still interfacing with each other.

Amazon SQS offers reliable, highly-scalable hosted queues for storing messages while they travel between applications or microservices. Amazon SQS lets you move data between distributed application components and helps you decouple these components. Amazon SWF is a web service that makes it easy to coordinate work across distributed application components.

Using RDS to utilize both on-premises servers and EC2 instances for your decoupled application and using DynamoDB to utilize both on-premises servers and EC2 instances for your decoupled application are incorrect as RDS and DynamoDB are database services.

Using Amazon Simple Decoupling Service to utilize both on-premises servers and EC2 instances for your decoupled application is incorrect because there is no such thing as Amazon Simple Decoupling Service.

References:

<https://aws.amazon.com/sqs/http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-welcome.html>

[Go back to Q277](#)

Answer to Q278: A

[Go back to Q278](#)

[Explanation to Q278](#)

NA

[Go back to Q278](#)

Answer to Q279: B

[Go back to Q279](#)

[Explanation to Q279](#)

NA

[Go back to Q279](#)

Answer to Q280: C

[Go back to Q280](#)

[Explanation to Q280](#)

In Amazon RDS, failover is automatically handled so that you can resume database operations as quickly as possible without administrative intervention if your primary database instance went down. When failing

over, Amazon RDS simply flips the canonical name record (CNAME) for your DB instance to point at the standby, which is in turn promoted to become the new primary.

The option that says: The IP address of the primary DB instance is switched to the standby DB instance is incorrect since IP addresses are per subnet, and subnets cannot span multiple AZs.

The option that says: The primary database instance will reboot is incorrect since in the event of a failure, there is no database to reboot with.

The option that says: A new database instance is created in the standby Availability Zone is incorrect since with multi-AZ enabled, you already have a standby database in another AZ.

References:

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/rds/faqs/>

[Go back to Q280](#)

Answer to Q281: D

[Go back to Q281](#)

Explanation to Q281

The correct answer is to 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.

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. If you have a bastion host in AWS, it is basically just an EC2 instance. It should be in a public subnet with

either a public or Elastic IP address with enough RDP or SSH access defined in the security group. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.

Deploying a Windows Bastion host on the corporate network that has RDP access to all EC2 instances in the VPC is incorrect since you do not deploy the Bastion host to your corporate network. It should be in the public subnet of a VPC.

Deploying a Windows Bastion host with an Elastic IP address in the private subnet, and restricting RDP access to the bastion from only the corporate public IP addresses is incorrect since it should be deployed in a public subnet, not a private subnet.

Deploying a Windows Bastion host with an Elastic IP address in the public subnet and allowing SSH access to the bastion from anywhere is incorrect. Since it is a Windows bastion, you should allow RDP access and not SSH as this is mainly used for Linux-based systems.

Reference:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

[Go back to Q281](#)

Answer to Q282: D

[Go back to Q282](#)

Explanation to Q282

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of

your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. OpsWorks has three offerings - AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise, and AWS OpsWorks Stacks.

Amazon Simple Workflow Service is incorrect because AWS SWF is a fully-managed state tracker and task coordinator in the Cloud. It does not let you leverage Chef recipes.

AWS Elastic Beanstalk is incorrect because this handles an application's deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. It does not let you leverage Chef recipes just like Amazon SWF. AWS CloudFormation is incorrect because this is a service that lets you create a collection of related AWS resources and provision them in a predictable fashion using infrastructure as code. It does not let you leverage Chef recipes just like Amazon SWF and AWS Elastic Beanstalk.

Reference:

<https://aws.amazon.com/opsworks/>

[Go back to Q282](#)

Answer to Q283: A

[Go back to Q283](#)

Explanation to Q283

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance,

and automatic scaling of throughput capacity makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

Hence, the correct answer is: Launch a DynamoDB table.

The option that says: Launch an Amazon RDS database with Read Replicas is incorrect because this is a relational database. This is not suitable to be used as a key-value store. A better option is to use DynamoDB as it supports both document and key-value store models.

The option that says: Use Amazon WorkDocs to store the document models is incorrect because Amazon WorkDocs simply enables you to share content, provide rich feedback, and collaboratively edit documents. It is not a key-value store like DynamoDB.

The option that says: Launch an Amazon Aurora Serverless database is incorrect because this type of database is not suitable to be used as a key-value store. Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora where the database will automatically start-up, shut down, and scale capacity up or down based on your application's needs. It enables you to run your database in the cloud without managing any database instances. It's a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads and not as a key-value store.

References:

<https://aws.amazon.com/dynamodb/>

<https://aws.amazon.com/nosql/key-value/>

[Go back to Q283](#)

Answer to Q284: C, E

[Go back to Q284](#)

Explanation to Q284

Server-side encryption is about data encryption at rest, i.e. , Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. If you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects.

You have three mutually exclusive options depending on how you choose to manage the encryption keys:

1. Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
2. Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
3. Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

The options that say: Before sending the data to Amazon S3 over HTTPS, encrypt the data locally first using your own encryption keys and Enable Server-Side Encryption on an S3 bucket to make use of AES-256 encryption are correct because these options are using client-side encryption and Amazon S3-Managed Keys (SSE-S3) respectively. Client-side encryption is the act of encrypting data before sending it to Amazon S3 while SSE-S3 uses AES-256 encryption.

Storing the data on EBS volumes with encryption enabled instead of using Amazon S3 and storing the data in encrypted EBS snapshots are incorrect because both options use EBS encryption and not S3. Enabling Server-Side Encryption on an S3 bucket to make use of AES-128 encryption is incorrect as S3 doesn't provide AES-128 encryption, only AES-256.

References:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

[Go back to Q284](#)

Answer to Q285: A, D

[Go back to Q285](#)

Explanation to Q285

In this scenario, the correct answers are:- Enable Multi-Factor Authentication- Assign an IAM role to the Amazon EC2 instance. Always remember that you should associate IAM roles to EC2 instances and not an IAM user, for the purpose of accessing other AWS services. IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor what they know), as well as for an authentication code from their AWS MFA device (the second factor what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can also be used to control access to AWS service APIs.

Storing the AWS Access Keys in the EC2 instance is incorrect because this is not recommended by AWS, as it can be compromised. Instead of storing access keys on an EC2 instance for use by applications that run on the instance and make AWS API requests, you can use an IAM role to provide temporary access keys for these applications.

Assigning an IAM user for each Amazon EC2 Instance is incorrect because there is no need to create an IAM user for this scenario since IAM roles already provide greater flexibility and easier management.

Storing the AWS Access Keys in ACM is incorrect because ACM is just a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. It is not used as a secure storage for your access keys.

References:

<https://aws.amazon.com/iam/details/mfa/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-foramazon-ec2.html>

[Go back to Q285](#)

Answer to Q286: A

[Go back to Q286](#)

Explanation to Q286

A new shard iterator is returned by every GetRecords request (as NextShardIterator), which you then use in the next GetRecords request (as ShardIterator). Typically, this shard iterator does not expire before you use it. However, you may find that shard iterators expire because you have not

called GetRecords for more than 5 minutes, or because you've performed a restart of your consumer application.

If the shard iterator expires immediately before you can use it, this might indicate that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data. This situation is more likely to happen if you have many shards. To solve this problem, increase the write capacity assigned to the shard table.

Hence, increasing the write capacity assigned to the shard table is the correct answer.

Upgrading the storage capacity of the DynamoDB table is incorrect because DynamoDB is a fully managed service which automatically scales its storage, without setting it up manually. The scenario refers to the write capacity of the shard table when it says that the DynamoDB table used by Kinesis does not have enough capacity to store the lease data.

Enabling In-Memory Acceleration with DynamoDB Accelerator (DAX) is incorrect because the DAX feature is primarily used for reading performance improvement of your DynamoDB table from milliseconds response time to microseconds. It does not have any relationship with Amazon Kinesis Data Stream in this scenario.

Using Amazon Kinesis Data Analytics to properly support the data analytics application instead of Kinesis Data Stream is incorrect because although Amazon Kinesis Data Analytics can support a data analytics application, it is still not a suitable solution for this issue. You simply need to increase the write capacity assigned to the shard table in order to rectify the problem which is why switching to Amazon Kinesis Data Analytics is not necessary.

Reference:

<https://docs.aws.amazon.com/streams/latest/dev/kinesis-record-processor-ddb.html>

<https://docs.aws.amazon.com/streams/latest/dev/troubleshooting-consumers.html>

[Go back to Q286](#)

Answer to Q287: C

[Go back to Q287](#)

Explanation to Q287

NA

[Go back to Q287](#)

Answer to Q288: A, B

[Go back to Q288](#)

Explanation to Q288

Amazon CloudWatch and Amazon Simple Notification Service (SNS) are correct. In this requirement, you can use Amazon CloudWatch to monitor the database and then Amazon SNS to send the emails to the Operations team. Take note that you should use SNS instead of SES (Simple Email Service) when you want to monitor your EC2 instances.

CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS, and on-premises servers.

SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

Amazon Simple Email Service is incorrect. SES is a cloud-based email sending service designed to send notification and transactional emails.

Amazon Simple Queue Service (SQS) is incorrect. SQS is a fully-managed message queuing service. It does not monitor applications nor send email notifications unlike SES.

Amazon EC2 Instance with a running Berkeley Internet Name Domain (BIND) Server is incorrect because BIND is primarily used as a Domain Name System (DNS) web service. This is only applicable if you have a private hosted zone in your AWS account. It does not monitor applications nor send email notifications.

References:

<https://aws.amazon.com/cloudwatch/>
<https://aws.amazon.com/sns/>

[Go back to Q288](#)

Answer to Q289: A

[Go back to Q289](#)

Explanation to Q289

NA

[Go back to Q289](#)

Answer to Q290: B

[Go back to Q290](#)

Explanation to Q290

Amazon EC2 uses public key cryptography to encrypt and decrypt login information. Public key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt

the data. The public and private keys are known as a key pair. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. On a Linux instance, the public key content is placed in an entry within `~/.ssh/authorized_keys`. This is done at boot time and enables you to securely access your instance using the private key instead of a password.

Custom EC2 password and EC2 Connection Strings are incorrect as both do not exist.

Access Keys is incorrect as these are used for API calls and not for logging in to EC2.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

[Go back to Q290](#)

Answer to Q291: C

[Go back to Q291](#)

Explanation to Q291

Perfect Forward Secrecy is a feature that provides additional safeguards against the eavesdropping of encrypted data, using a unique random session key. This prevents the decoding of captured data, even if the secret long-term key is compromised.

CloudFront and Elastic Load Balancing are the two AWS services that support Perfect Forward Secrecy.

Hence, the correct answer is: CloudFront and Elastic Load Balancing. EC2 and S3, CloudTrail and CloudWatch, and Trusted Advisor and GovCloud are incorrect since these services do not use Perfect Forward Secrecy.

SSL/TLS is commonly used when you have sensitive data travelling through the public network.

References:

<https://aws.amazon.com/about-aws/whats-new/2014/02/19/elastic-load-balancing-perfect-forward-secrecy-and-more-new-security-features/>

https://d1.awsstatic.com/whitepapers/Security/Secure_content_delivery_with_CloudFront_whitepaper.pdf

[Go back to Q291](#)

Answer to Q292: B

[Go back to Q292](#)

Explanation to Q292

The best way to implement a bastion host is to create a small EC2 instance which should only have a security group from a specific IP address for maximum security. This will block any SSH Brute Force attacks on your bastion host. It is also recommended to use a small instance rather than a large one because this host will only act as a jump server to connect to other instances in your VPC and nothing else.

Therefore, there is no point of allocating a large instance simply because it doesn't need that much computing power to process SSH (port 22) or RDP (port 3389) connections. It is possible to use SSH with an ordinary user ID and a pre-configured password as credentials, but it is more secure to use public key pairs for SSH authentication for better security.

Hence, the right answer for this scenario is the option that says: 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.

Creating a large EC2 instance with a security group which only allows access on port 22 using your own pre-configured password and creating a small EC2 instance with a security group which only allows access on port 22 using your own pre-configured password are incorrect because even though you have your own pre-configured password, the SSH connection can still be accessed by anyone over the Internet, which poses as a security vulnerability.

The option that says: 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 is incorrect because you don't need a large instance for a bastion host as it does not require much CPU resources.

References:

<https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html>

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/>

[Go back to Q292](#)

Answer to Q293: A

[Go back to Q293](#)

Explanation to Q293

In this scenario, the best option is to use Amazon S3. It's a simple storage service that offers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.

Multiple Amazon EBS volume with snapshots and Multiple instance stores are incorrect because these services do not provide durable storage.

Amazon S3 Glacier Deep Archive is incorrect because this is mainly used for data archives with data retrieval times that can take more than 12 hours. Hence, it is not suitable for the transcription service where the data are stored and frequently accessed.

Reference:

<https://aws.amazon.com/s3/faqs/>

[Go back to Q293](#)

Answer to Q294: D

[Go back to Q294](#)

Explanation to Q294

To allow the custom port, you must change the Inbound Rules in your Security Group to allow traffic coming from the mobile devices. Security Groups usually control the list of ports that can be used by your EC2 instances and the NACLs control which network or list of IP addresses can connect to your whole VPC.

When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group. By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound

traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.

The option that says: Open the custom port on the Security Group. Your EC2 instances will be able to use this port after 60 minutes and Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port after a reboot are both incorrect because any changes to the Security Groups or Network Access Control Lists are applied immediately and not after 60 minutes or after the instance reboot.

The option that says: Open the custom port on the Network Access Control List of your VPC. Your EC2 instances will be able to use this port immediately is incorrect because the scenario says that VPC is using a default configuration. Since by default, Network ACL allows all inbound and outbound IPv4 traffic, then there is no point of explicitly allowing the port in the Network ACL. Security Groups, on the other hand, does not allow incoming traffic by default, unlike Network ACL.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security_Groups.html

[Go back to Q294](#)

Answer to Q295: B

[Go back to Q295](#)

Explanation to Q295

You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. Automating snapshot management helps you to:-

Protect valuable data by enforcing a regular backup schedule.- Retain backups as required by auditors or internal compliance.- Reduce storage costs by deleting outdated backups.

Combined with the monitoring features of Amazon CloudWatch Events and AWS CloudTrail, Amazon DLM provides a complete backup solution for EBS volumes at no additional cost.

Hence, using Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation of EBS snapshots is the correct answer as it is the fastest and most cost-effective solution that provides an automated way of backing up your EBS volumes.

The option that says: 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 is incorrect because even though this is a valid solution, you would still need additional time to create a scheduled job that calls the "create-snapshot" command. It would be better to use Amazon Data Lifecycle Manager (Amazon DLM) instead as this provides you the fastest solution which enables you to automate the creation, retention, and deletion of the EBS snapshots without having to write custom shell scripts or creating scheduled jobs.

Setting your Amazon Storage Gateway with EBS volumes as the data source and storing the backups in your on-premises servers through the storage gateway is incorrect as the Amazon Storage Gateway is used only for creating a backup of data from your on-premises server and not from the Amazon Virtual Private Cloud.

Using an EBS-cycle policy in Amazon S3 to automatically back up the EBS volumes is incorrect as there is no such thing as EBS-cycle policy in Amazon S3.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

[Go back to Q295](#)

Answer to Q296: D

[Go back to Q296](#)

Explanation to Q296

AWS Security Token Service (AWS STS) is the service that you can use to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use.

In this diagram, IAM user Alice in the Dev account (the role-assuming account) needs to access the Prod account (the role-owning account).

Here is how it works:

. Alice in the Dev account assumes an IAM role (WriteAccess) in the Prod account by calling AssumeRole. STS returns a set of temporary security credentials. Alice uses the temporary security credentials to access services and resources in the Prod account. Alice could, for example, make calls to Amazon S3 and Amazon EC2, which are granted by the WriteAccess role.

Using AWS Cognito to issue JSON Web Tokens (JWT) is incorrect because the Amazon Cognito service is primarily used for user authentication and not for providing access to your AWS resources. A JSON Web Token (JWT) is meant to be used for user authentication and session management.

Using AWS SSO is incorrect because although the AWS SSO service uses STS, it does not issue short-lived credentials by itself. AWS Single Sign-On

(SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

The option that says All of the given options are correct is incorrect as only STS can provide temporary security credentials.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

[Go back to Q296](#)

Answer to Q297: B, E

[Go back to Q297](#)

Explanation to Q297

Amazon S3 Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. Amazon Glacier is designed to store data that is infrequently accessed. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

Storing cached session data is incorrect because this is the main use case for ElastiCache and not Amazon Glacier.

The option that says: Used for active database storage is incorrect because you should use RDS or DynamoDB for your active database storage as S3, in general, is used for storing your data or files.

The option that says: Used as a data warehouse is incorrect because storing it for data warehousing is the main use case of Amazon Redshift. It does not meet the requirement of being able to archive your infrequently accessed data. You can use S3 standard instead for frequently accessed data or Glacier for infrequently accessed data and archiving.

It is advisable to transition the standard data to infrequent access first then transition it to Amazon Glacier. You can specify in the lifecycle rule the time it will sit in standard tier and infrequent access. You can also delete the objects after a certain amount of time.

In transitioning S3 standard to Glacier you need to tell S3 which objects are to be archived to the new Glacier storage option, and under what conditions.

You do this by setting up a lifecycle rule using the following elements: A prefix to specify which objects in the bucket are subject to the policy. A relative or absolute time specifier and a time period for transitioning objects to Glacier. The time periods are interpreted with respect to the object's creation date.

They can be relative (migrate items that are older than a certain number of days) or absolute (migrate items on a specific date) An object age at which the object will be deleted from S3. This is measured from the original PUT of the object into the service, and the clock is not reset by a transition to Glacier.

You can create a lifecycle rule in the AWS Management Console.

Reference:

<https://aws.amazon.com/glacier/faqs/>

[Go back to Q297](#)

Answer to Q298: B

[Go back to Q298](#)

Explanation to Q298

SNI Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

Amazon CloudFront delivers your content from each edge location and offers the same security as the Dedicated IP Custom SSL feature. SNI Custom SSL works with most modern browsers, including Chrome version 6 and later (running on Windows XP and later or OS X 10.5.7 and later), Safari version 3 and later (running on Windows Vista and later or Mac OS X 10.5.6. and later), Firefox 2.0 and later, and Internet Explorer 7 and later (running on Windows Vista and later). Some users may not be able to access your content because some older browsers do not support SNI and will not be able to establish a connection with CloudFront to load the HTTPS version of your content. If you need to support non-SNI compliant browsers for HTTPS content, it is recommended to use the Dedicated IP Custom SSL feature.

Using Server Name Indication (SNI) on your Classic Load Balancer by adding multiple SSL certificates to allow multiple domains to serve SSL traffic is incorrect because a Classic Load Balancer does not support Server Name Indication (SNI). You must use an Application Load Balancer instead or a CloudFront web distribution to allow the SNI feature.

Using an Elastic IP and uploading multiple 3rd party certificates in your Classic Load Balancer using the AWS Certificate Manager is incorrect because just like in the above, a Classic Load Balancer does not support Server Name Indication (SNI) and the use of an Elastic IP is not a suitable solution to allow multiple domains to serve SSL traffic. You must use Server Name Indication (SNI).

The option that says: It is not possible to allow multiple domains to serve SSL traffic over the same IP address in AWS is incorrect because AWS does support the use of Server Name Indication (SNI).

References:

<https://aws.amazon.com/about-aws/whats-new/2014/03/05/amazon-cloudfront-announces-sni-custom-ssl/>

<https://aws.amazon.com/blogs/security/how-to-help-achieve-mobile-app-transport-security-compliance-by-using-amazon-cloudfront-and-aws-certificate-manager/>

[Go back to Q298](#)

Answer to Q299: D

[Go back to Q299](#)

Explanation to Q299

In this scenario, the main culprit is that 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.

The option that says: The sqsSendMessage attribute of the SQS queue is configured to 50 is incorrect as there is no sqsSendMessage attribute in SQS.

The option that says: There is a bug in the application is a valid answer but since the scenario did not mention that the EC2 instances deleted the processed messages, the most likely cause of the problem is that the application does not issue a delete command to the SQS queue as mentioned above.

The option that says: 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 is incorrect as SQS does not automatically delete the messages.

Reference:

<https://aws.amazon.com/sqs/faqs/>

[Go back to Q299](#)

Answer to Q300: A, B

[Go back to Q300](#)

Explanation to Q300

NA

[Go back to Q300](#)

Answer to Q301: A

[Go back to Q301](#)

Explanation to Q301

NA

[Go back to Q301](#)

Answer to Q302: A

[Go back to Q302](#)

Explanation to Q302

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

Setting up an Application Load Balancers that will automatically route the traffic to the proper AWS region is incorrect because Elastic Load Balancers distribute traffic among EC2 instances across multiple Availability Zones but not across AWS regions.

Setting up a new CloudFront web distribution with the geo-restriction feature enabled is incorrect because the CloudFront geo-restriction feature is primarily used to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution. It does not let you choose the resources that serve your traffic based on the geographic location of your users, unlike the Geolocation routing policy in Route 53. Using Route 53 Weighted Routing policy is incorrect because this is not a suitable solution to meet the requirements of this scenario. It just lets you associate multiple resources with a single domain name (techrad.io) or subdomain name (forums.techrad.io) and choose how much traffic is routed to each resource. You must use a Geolocation routing policy instead.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/geolocation-routing-policy>

[Go back to Q302](#)

Answer to Q303: B, E

[Go back to Q303](#)

Explanation to Q303

Using an Elastic Load Balancer is an ideal solution for adding elasticity to your application. Alternatively, you can also create a policy in Route 53, such as a Weighted routing policy, to evenly distribute the traffic to 2 or more EC2 instances. Hence, setting up two EC2 instances and then put them behind an Elastic Load balancer (ELB) and setting up two EC2 instances and using Route 53 to route traffic based on a Weighted Routing Policy are the correct answers.

Setting up an S3 Cache in front of the EC2 instance is incorrect because doing so does not provide elasticity and scalability to your EC2 instances.

Setting up an AWS WAF behind your EC2 Instance is incorrect because AWS WAF is a web application firewall that helps protect your web applications from common web exploits. This service is more on providing security to your applications.

Setting up two EC2 instances deployed using Launch Templates and integrated with AWS Glue is incorrect because AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It does not provide scalability or elasticity to your instances.

References:

<https://aws.amazon.com/elasticloadbalancing>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide>Welcome.html>

[Go back to Q303](#)

Answer to Q304: D

[Go back to Q304](#)

Explanation to Q304

Elastic Load Balancing supports three types of load balancers. You can select the appropriate load balancer based on your application needs.

If you need flexible application management and TLS termination, then we recommend that you use Application Load Balancer. If extreme performance and static IP is needed for your application, then we recommend that you use Network Load Balancer. If your application is built within the EC2 Classic network, then you should use Classic Load Balancer.

An Application Load Balancer functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply, and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic. Routing is performed independently for each target group, even when a target is registered with multiple target groups.

Application Load Balancers support path-based routing, host-based routing and support for containerized applications hence, Application Load Balancer is the correct answer.

Network Load Balancer, Classic Load Balancer, and either a Classic Load Balancer or a Network Load Balancer are all incorrect as none of these support path-based routing and host-based routing, unlike an Application Load Balancer.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-benefits>

<https://aws.amazon.com/elasticloadbalancing/faqs/>

[Go back to Q304](#)

Answer to Q305: C

[Go back to Q305](#)

Explanation to Q305

The best practice in handling API Credentials is to create a new role in the Identity Access Management (IAM) service and then assign it to a specific EC2 instance. In this way, you have a secure and centralized way of storing and managing your credentials.

Storing the API credentials in the EC2 instance, adding the API Credentials in the Security Group and assigning it to the EC2 instance, and storing the API credentials in a bastion host are incorrect because it is not secure to store nor use the API credentials from an EC2 instance. You should use IAM service instead.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

[Go back to Q305](#)

Answer to Q306: C

[Go back to Q306](#)

Explanation to Q306

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules like your security groups in order to add an additional layer of security to your VPC.

Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found.

The option that says: Network ACL Rules are evaluated by rule number, from highest to lowest and are executed immediately when a matching allow/deny rule is found is incorrect since rules are evaluated from lowest to highest, not the other way around.

The option that says: By default, all Network ACL Rules are evaluated before any traffic is allowed or denied is incorrect because the Network ACL Rules are evaluated by rule number, from lowest to highest, and executed immediately when a matching allow/deny rule is found.

The option that says: Network ACL Rules are evaluated by rule number, from lowest to highest, and executed after all rules are checked for conflicting allow/deny rules is incorrect since rules are executed immediately when a match is found and not after all rules are checked for conflicting allow/deny rules.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[Go back to Q306](#)

Answer to Q307: B, D

[Go back to Q307](#)

Explanation to Q307

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

Amazon S3 supports the following destinations where it can publish events:

1. Amazon Simple Notification Service (Amazon SNS) topic - A web service that coordinates and manages the delivery or sending of messages to subscribe endpoints or clients.
2. Amazon Simple Queue Service (Amazon SQS) queue - Offers reliable and scalable hosted queues for storing messages as they travel between computer.
3. AWS Lambda - AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function
4. Kinesis is incorrect because this is used to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly

to new information, and not used for event notifications.

You must use SNS, SQS or Lambda.

SES is incorrect because this is mainly used for sending emails designed to help digital marketers and application developers send marketing, notification, and transactional emails, and not for sending event notifications from S3. You must use SNS, SQS or Lambda. SWF is incorrect because this is mainly used to build applications that use Amazon's cloud to coordinate work across distributed components and not used to trigger event notifications from S3. You must use SNS, SQS or Lambda.

Here is what you need to do in order to start using this new feature with your application. Create the queue, topic, or Lambda function (which I'll call the target for brevity) if necessary. Grant S3 permission to publish to the target or invoke the Lambda function. For SNS or SQS, you do this by applying an appropriate policy to the topic or the queue. For Lambda, you must create and supply an IAM role, then associate it with the Lambda function. Arrange for your application to be invoked in response to activity on the target. As you will see in a moment, you have several options here. Set the buckets Notification Configuration to point to the target.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

[Go back to Q307](#)

Answer to Q308: B

[Go back to Q308](#)

[Explanation to Q308](#)

Memory Usage is a metric not available by default in CloudWatch. You need to add a custom metric for it to work.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>

[Go back to Q308](#)

Answer to Q309: A

[Go back to Q309](#)

Explanation to Q309

Use an active-passive failover configuration when you want a primary resource or group of resources to be available majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route 53 responds to DNS queries using the secondary record.

You can configure a health check that monitors an endpoint that you specify either by IP address or by domain name. At regular intervals that you specify, Route 53 submits automated requests over the Internet to your application, server, or other resource to verify that it's reachable, available, and functional. Optionally, you can configure the health check to

make requests like those that your users make, such as requesting a web page from a specific URL.

When Route 53 checks the health of an endpoint, it sends an HTTP, HTTPS, or TCP request to the IP address and port that you specified when you created the health check. For a health check to succeed, your router and firewall rules must allow inbound traffic from the IP addresses that the Route 53 health checkers use.

Hence, the correct answer is: 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.

The option that says: 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 is incorrect because Weighted routing simply lets you associate multiple resources with a single domain name (techrad.io) or subdomain name (blog.techrad.io) and choose how much traffic is routed to each resource.

This can be useful for a variety of purposes, including load balancing and testing new versions of software, but not for a failover configuration. Remember that the scenario says that the solution should automatically route the live traffic to the disaster recovery (DR) environment only if the primary application stack experiences an outage. This configuration is incorrectly distributing the traffic on both the primary and DR environment.

The option that says: 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 is incorrect because setting up a CloudWatch Alarm and using the Route 53 API is not applicable nor useful at all in this scenario. Remember that CloudWatch Alarms are primarily used for monitoring CloudWatch metrics. You must use a Failover routing policy instead.

The option that says: 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 is incorrect because the Amazon CloudWatch Events service is commonly used to deliver a near real-time stream of system events that describe changes in some Amazon Web Services (AWS) resources. There is no direct way for CloudWatch Events to monitor the status of your Route 53 endpoints. You must configure a health check and a failover configuration in Route 53 instead to satisfy the requirement in this scenario.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-types.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-router-firewall-rules.html>

[Go back to Q309](#)

Answer to Q310: C

[Go back to Q310](#)

Explanation to Q310

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

DynamoDB is incorrect. DynamoDB is a NoSQL database which is based on key-value pairs used for fast processing of small data that dynamically grows and changes. But if you need to scan large amounts of data (i.e. a lot of keys all in one query), the performance will not be optimal.

ElastiCache is incorrect because this is used to increase the performance, speed and redundancy with which applications can retrieve data by providing an in-memory database caching system, and not for database analytical processes.

RDS is incorrect because this is mainly used for On-Line Transaction Processing (OLTP) applications and not for Online Analytics Processing (OLAP).

References:

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

<https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html>

[Go back to Q310](#)

Answer to Q311: A

[Go back to Q311](#)

Explanation to Q311

In this scenario, it is best to create 2 separate SQS queues for each type of members. The SQS queues for the premium members can be polled first by the EC2 Instances and once completed, the messages from the free members can be processed next.

The option that says: 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 is incorrect as you cannot set a priority to individual items in the SQS queue.

Using Amazon Kinesis to process the photos and generate the video montage in real time is incorrect as Amazon Kinesis is used to process streaming data and it is not applicable in this scenario.

Using Amazon S3 to store and process the photos and then generating the video montage afterwards is incorrect as Amazon S3 is used for durable storage and not for processing data.

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-best-practices.html>

[Go back to Q311](#)

Answer to Q312: A, C

[Go back to Q312](#)

Explanation to Q312

Alias with a type "AAAA" record set and Alias with a type "A" record set are correct. To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS. It's like a CNAME record, but you

can create an alias record both for the root domain, such as techrad.io, and for subdomains, such as portal.techrad.io. (You can create CNAME records only for subdomains.) To enable IPv6 resolution, you would need to create a second resource record, techrad.io ALIAS AAAA -> myelb.us-west-2.elb.amazonaws.com, this is assuming your Elastic Load Balancer has IPv6 support.

Non-Alias with a type "A" record set is incorrect because you only use Non-Alias with a type A record set for IP addresses.

Alias with a type "CNAME" record set is incorrect because you can't create a CNAME record at the zone apex. For example, if you register the DNS name techrad.io, the zone apex is techrad.io.

Alias with a type of MX record set is incorrect because an MX record is primarily used for mail servers. It includes a priority number and a domain name, for example: 10 mailserver.techrad.io.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

[Go back to Q312](#)

Answer to Q313: A, C

[Go back to Q313](#)

[Explanation to Q313](#)

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM). In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance and help protect your databases against DB instance failure and Availability Zone disruption.

Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention. The high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a Read Replica.

Amazon RDS automatically performs a failover in the event of any of the following:

1. Loss of availability in primary Availability Zone
2. Loss of network connectivity to primary
3. Compute unit failure on primary
4. Storage failure on primary

The following options are incorrect because all these scenarios do not affect the primary database. Automatic failover only occurs if the primary database is the one that is affected.- Storage failure on secondary DB

instance- In the event of Read Replica failure- Compute unit failure on secondary DB instance

References:

<https://aws.amazon.com/rds/details/multi-az/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

[Go back to Q313](#)

Answer to Q314: B

[Go back to Q314](#)

Explanation to Q314

NA

[Go back to Q314](#)

Answer to Q315: B

[Go back to Q315](#)

Explanation to Q315

AWS Secrets Manager is an AWS service that makes it easier for you to manage secrets. Secrets can be database credentials, passwords, third-party API keys, and even arbitrary text. You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs.

In the past, when you created a custom application that retrieves information from a database, you typically had to embed the credentials (the secret) for accessing the database directly in the application. When it came time to rotate the credentials, you had to do much more than just create new credentials. You had to invest time to update the application to use the new credentials. Then you had to distribute the updated application. If you had multiple applications that shared credentials and you missed updating one of them, the application would break. Because of this risk, many customers have chosen not to regularly rotate their credentials, which effectively substitutes one risk for another.

Secrets Manager enables you to replace hardcoded credentials in your code (including passwords), with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure that the secret can't be compromised by someone examining your code, because the secret simply isn't there. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a schedule that you specify. This enables you to replace long-term secrets with short-term ones, which helps to significantly reduce the risk of compromise.

Hence, the most appropriate solution for this scenario is: Use AWS Secrets Manager to store and encrypt the database credentials, API keys, and other secrets. Enable automatic rotation for all the credentials.

The option that says: 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 is incorrect because Systems Manager Parameter Store doesn't rotate its parameters by default.

The option that says: Store the database credentials, API keys, and other secrets to AWS ACM is incorrect because it is just a managed private CA service that helps you easily and securely manage the lifecycle of your private certificates to allow SSL communication to your application. This is not a suitable service to store database or any other confidential credentials.

The option that says: Store the database credentials, API keys, and other secrets in AWS KMS is incorrect because this only makes it easy for you to create and manage encryption keys and control the use of encryption across a wide range of AWS services. This is primarily used for encryption and not for hosting your credentials.

References:

<https://aws.amazon.com/secrets-manager/>

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-using-aws-secrets-manager/>

[Go back to Q315](#)

Answer to Q316: A

[Go back to Q316](#)

Explanation to Q316

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

Writing a python script that queries the EC2 API for each instance status check, writing a shell script that periodically shuts down and starts instances based on certain stats, and buying and implementing a third party monitoring tool are all incorrect because it is unnecessary to go through such lengths when CloudWatch Alarms already has such a feature for you, offered at a low cost.

Reference:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

[Go back to Q316](#)

Answer to Q317: D, E

[Go back to Q317](#)

Explanation to Q317

In this scenario, you have two VPCs which have peering connections with each other. Note that a VPC peering connection does not support edge to edge routing. This means that if either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:- A VPN connection or an AWS Direct Connect connection to a corporate network- An Internet connection through an Internet gateway- An Internet connection in a private subnet through a NAT device- A gateway VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.- (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.

For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B.

Hence, this means that you cannot use VPC-2 to extend the peering relationship that exists between VPC-1 and the on-premises network. For example, traffic from the corporate network can't directly access VPC-1 by

using the VPN connection or the AWS Direct Connect connection to VPC-2, which is why the following options are incorrect:

- Use the AWS VPN CloudHub to create a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- Establish a hardware VPN over the Internet between VPC-2 and the on-premises network.
- Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

You can do the following to provide a highly available, fault-tolerant network connection:

- Establish a hardware VPN over the Internet between the VPC and the on-premises network.
- Establish another AWS Direct Connect connection and private virtual interface in the same AWS region.

References:

<https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-to-edge-vgw>

<https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/>

<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>

[Go back to Q317](#)

Answer to Q318: C, E

[Go back to Q318](#)

Explanation to Q318

First, the Network ACL should be properly set to allow communication between the two subnets. The security group should also be properly configured so that your web server can communicate with the database server.

Hence, these are the correct answers:

1 Check if all security groups are set to allow the application host to communicate to the database on the right port and protocol.

2 Check the Network ACL if it allows communication between the two subnets.

The option that says: Check if both instances are the same instance class is incorrect because the EC2 instances do not need to be of the same class in order to communicate with each other.

The option that says: Check if the default route is set to a NAT instance or Internet Gateway (IGW) for them to communicate is incorrect because an Internet gateway is primarily used to communicate to the Internet.

The option that says: Ensure that the EC2 instances are in the same Placement Group is incorrect because Placement Group is mainly used to provide low-latency network performance necessary for tightly-coupled node-to-node communication.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

[Go back to Q318](#)

Answer to Q319: C

[Go back to Q319](#)

Explanation to Q319

Creating snapshots of the EBS Volumes is correct. You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all the information needed to restore your data (from the moment the snapshot was taken) to a new EBS volume.

EBS-backed EC2 instances is incorrect since running an EBS-backed EC2 instance does not relate to your problem as you are already running a few of them in the first place.

Using Disk Mirroring, which is also known as RAID 1, that replicates data to two or more disks/EBS Volumes is incorrect. Disk mirroring is not an efficient and cost-optimized solution for your problem. You should use EBS snapshots instead.

Launching the EBS Volumes to a Placement Group which will automatically back up your data is incorrect. A placement group is a logical grouping of instances within a single Availability Zone (AZ) that allows low-latency communication between instances. Hence, this is not an efficient way to back up data.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

[Go back to Q319](#)

Answer to Q320: D, E

[Go back to Q320](#)

Explanation to Q320

An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application. You can also use them for throughput-intensive applications that perform continuous disk scans. EBS volumes persist independently from the running life of an EC2 instance.

Here is a list of important information about EBS Volumes:

- When you create an EBS volume in an Availability Zone, it is automatically replicated within that zone to prevent data loss due to a failure of any single hardware component.- An EBS volume can only be attached to one EC2 instance at a time.
- After you create a volume, you can attach it to any EC2 instance in the same Availability Zone- An EBS volume is off-instance storage that can persist independently from the life of an instance. You can specify not to terminate the EBS volume when you terminate the EC2 instance during instance creation.
- 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.- Amazon EBS encryption uses 256-bit Advanced Encryption Standard algorithms (AES-256)- EBS Volumes offer 99.999% SLA.

The option that says: 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 is incorrect because when you create an EBS volume in an Availability Zone, it is automatically replicated within that zone only, and not on a separate AWS region, to prevent data loss due to a failure of any single hardware component.

The option that says: EBS volumes can be attached to any EC2 Instance in any Availability Zone is incorrect as EBS volumes can only be attached to an EC2 instance in the same Availability Zone.

The option that says: 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 is almost correct. But instead of storing the volume to Amazon RDS, the EBS Volume snapshots are sent to Amazon S3.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>

<https://aws.amazon.com/ebs/features/>

[Go back to Q320](#)

Answer to Q321: C

[Go back to Q321](#)

Explanation to Q321

Instance metadata is the data about your instance that you can use to configure or manage the running instance. You can get the instance ID, public keys, public IP address and many other information from the

instance metadata by firing a URL command in your instance to this URL:`http://169.254.169.254/latest/meta-data/Instance` user data is incorrect because this is mainly used to perform common automated configuration tasks and run scripts after the instance starts.

Resource tags is incorrect because these are labels that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.

Amazon Machine Image is incorrect because this mainly provides the information required to launch an instance, which is a virtual server in the cloud.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.htm>

[Go back to Q321](#)

Answer to Q322: D

[Go back to Q322](#)

Explanation to Q322

Server-side encryption protects data at rest. If you use Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3), Amazon S3 will encrypt each object with a unique key and as an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

If you need server-side encryption for all the objects that are stored in a bucket, use a bucket policy.

However, if you chose to use server-side encryption with customer-provided encryption keys (SSE-C), you must provide encryption key information using the following request headers:`x-amz-server-side-encryption-customer-algorithm``x-amz-server-side-encryption-customer-key``x-amz-server-side-encryption-customer-key-MD5`Hence, using the `x-amz-server-side-encryption` header is correct as this is the one being used for Amazon S3-Managed Encryption Keys (SSE-S3).

All other options are incorrect since they are used for SSE-C.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryption-CustomerKeys.html>

[Go back to Q322](#)

Answer to Q323: C

[Go back to Q323](#)

Explanation to Q323

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, API Gateway, CloudFront or an Application Load Balancer

responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You also can configure CloudFront to return a custom error page when a request is blocked.

At the simplest level, AWS WAF lets you choose one of the following behaviors:

1. Allow all requests except the ones that you specify: This is useful when you want CloudFront or an Application Load Balancer to serve content for a public website, but you also want to block requests from attackers.
2. Block all requests except the ones that you specify : This is useful when you want to serve content for a restricted website whose users are readily identifiable by properties in web requests, such as the IP addresses that they use to browse to the website.
- 3.Count the requests that match the properties that you specify: When you want to allow or block requests based on new properties in web requests, you first can configure AWS WAF to count the requests that match those properties without allowing or blocking those requests. This lets you confirm that you didn't accidentally configure AWS WAF to block all the traffic to your website. When you're confident that you specified the correct properties, you can change the behavior to allow or block requests.

Hence, the correct answer in this scenario is: 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.

Using Amazon GuardDuty to prevent any further SQL injection and cross-site scripting attacks in your application is incorrect because Amazon GuardDuty is just a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Using AWS Firewall Manager to set up security rules that block SQL injection and cross-site scripting attacks, then associating the rules to the Application Load Balancer is incorrect because the AWS Firewall Manager

just simplifies your AWS WAF and AWS Shield Advanced administration and maintenance tasks across multiple accounts and resources.

Blocking all the IP addresses where the SQL injection and cross-site scripting attacks originated using the Network Access Control List is incorrect because this is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. NACLs are not effective in blocking SQL injection and cross-site scripting attacks

References:

<https://aws.amazon.com/waf/https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

[Go back to Q323](#)

Answer to Q324: D

[Go back to Q324](#)

Explanation to Q324

You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. The attributes of a network interface follow it as it's attached or detached from an instance and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance.

If one of your instances serving a function fails, its network interface can be attached to a replacement or hot standby instance pre-configured for the same role in order to rapidly recover the service. For example, you can use a network interface as your primary or secondary network interface to a critical service such as a database instance or a NAT instance.

If the instance fails, you (or more likely, the code running on your behalf) can attach the network interface to a hot standby instance. Because the interface maintains its private IP addresses, Elastic IP addresses, and MAC address, network traffic begins flowing to the standby instance as soon as you attach the network interface to the replacement instance. Users experience a brief loss of connectivity between the time the instance fails and the time that the network interface is attached to the standby instance, but no changes to the VPC route table or your DNS server are required.

An elastic network interface (ENI) is a logical networking component in a VPC that represents a virtual network card. You can attach a network interface to an EC2 instance in the following ways:

1. When it's running (hot attach)
2. When it's stopped (warm attach)When the instance is being launched (cold attach).Therefore, attaching an ENI to an instance when it is stopped is the correct answer.

Attaching an ENI to an instance during the launch process is incorrect because this describes a "cold attach" scenario.

Attaching an ENI to an instance when it is running is incorrect because this describes a "hot attach" scenario.

Attaching an ENI to an instance when it is idle is incorrect because there is no specific name for attaching an ENI to an idle EC2 instance.

References:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#attach_eni_launch

<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-detach-or-delete-eni/>

[Go back to Q324](#)

Answer to Q325: A

[Go back to Q325](#)

Explanation to Q325

A Content Delivery Network (CDN) is a critical component of nearly any modern web application. It used to be that CDN merely improved the delivery of content by replicating commonly requested files (static content) across a globally distributed set of caching servers. However, CDNs have become much more useful over time.

For caching, a CDN will reduce the load on an application origin and improve the experience of the requestor by delivering a local copy of the content from a nearby cache edge or Point of Presence (PoP). The application origin is off the hook for opening the connection and delivering the content directly as the CDN takes care of the heavy lifting. The result is that the application origins don't need to scale to meet demands for static content.

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services.

Amazon S3 offers a highly durable, scalable, and secure destination for backing up and archiving your critical data. This is the correct option as the start-up company is looking for a durable storage to store the audio and text files. In addition, ElastiCache is only used for caching and not specifically as a Global Content Delivery Network (CDN).Using Amazon

Redshift as the data storage and CloudFront as the CDN is incorrect as Amazon Redshift is usually used as a Data Warehouse.

Using Amazon S3 Glacier as the data storage and ElastiCache as the CDN is incorrect as Amazon S3 Glacier is usually used for data archives.

Using multiple EC2 instance stores for data storage and ElastiCache as the CDN is incorrect as data stored in an instance store is not durable.

References:

<https://aws.amazon.com/s3/><https://aws.amazon.com/caching/cdn/>

[Go back to Q325](#)

Answer to Q326: A

[Go back to Q326](#)

Explanation to Q326

When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY and UNLOAD traffic between your cluster and your data repositories through your Amazon VPC. By using Enhanced VPC Routing, you can use standard VPC features, such as VPC security groups, network access control lists (ACLs), VPC endpoints, VPC endpoint policies, internet gateways, and Domain Name System (DNS) servers. Hence, enabling Enhanced VPC routing on your Amazon Redshift cluster is the correct answer.

You use these features to tightly manage the flow of data between your Amazon Redshift cluster and other resources. When you use Enhanced VPC Routing to route traffic through your VPC, you can also use VPC flow logs to monitor COPY and UNLOAD traffic. If Enhanced VPC Routing is not enabled,

Amazon Redshift routes traffic through the Internet, including traffic to other services within the AWS network.

Enabling Audit Logging in your Amazon Redshift cluster is incorrect because the Audit Logging feature is primarily used to get the information about the connection, queries, and user activities in your Redshift cluster.

Using the Amazon Redshift Spectrum feature is incorrect because this is primarily used to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required.

Creating a new flow log that tracks the traffic of your Amazon Redshift cluster is incorrect because, by default, you cannot create a flow log for your Amazon Redshift cluster. You must enable Enhanced VPC Routing and set up the required VPC configuration.

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html>

[Go back to Q326](#)

Answer to Q327: A, D

[Go back to Q327](#)

Explanation to Q327

You can secure the privacy of your data in AWS, both at rest and in-transit, through encryption. If your data is stored in EBS Volumes, you can enable EBS Encryption and if it is stored on Amazon S3, you can enable client-side and server-side encryption.

Public Data Set Volume Encryption is incorrect as public data sets are designed to be publicly accessible.

EBS On-Premises Data Encryption and S3 On-Premises Data Encryption are both incorrect as there is no such thing as On-Premises Data Encryption for S3 and EBS as these services are in the AWS cloud and not on your on-premises network.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html>

[Go back to Q327](#)

Answer to Q328: A

[Go back to Q328](#)

Explanation to Q328

Since you are using an EC2 instance with an Instance store, its data is ephemeral which means that it will be erased once the instance is stopped or terminated. You may argue that the instance was only shut down but remember that the Operating system shutdown commands always terminate an instance store-backed instance.

That is why the right answer is the option that says: The EC2 instance was using an instance store hence, data will be erased when the instance is stopped or terminated.

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists.

However, data in the instance store is lost under any of the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

Therefore, do not rely on instance store for valuable, long-term data. Instead, use more durable data storage such as Amazon S3, Amazon EBS, or Amazon EFS. When you stop or terminate an instance, every block of storage in the instance store is reset. Hence, your data cannot be accessed through the instance store of another instance.

If you create an AMI from an instance, the data on its instance store volumes aren't preserved and aren't present on the instance store volumes of the instances that you launch from the AMI. You can specify instance store volumes for an instance only when you launch it. You can't detach an instance store volume from one instance and attach it to a different instance.

The option that says: The EC2 instance was using EBS-backed root volumes hence, the data will be erased when the instance is shut down or stopped is incorrect because the data will persist if you use an EBS-backed root volume.

The option that says: AWS automatically erased the data due to a virus found on the EC2 instance is incorrect because based on the AWS Shared Responsibility model, AWS will only manage the underlying resources that the services are using and not your actual data. Hence, it is highly unlikely that AWS will automatically erase your data due to a virus.

The option that says: The EC2 instance has been hacked is incorrect because although it is remotely possible that someone got hold of your AWS security credentials and deletes your data, this reason is still far-

fetched and quite unlikely to happen. Based on the given scenario, the stopping of the instance is one key attribute which we can link to its use of Instance Store volumes.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Storage.html>

[Go back to Q328](#)

Answer to Q329: C

[Go back to Q329](#)

Explanation to Q329

Amazon API Gateway provides throttling at multiple levels including global and by a service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs and configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds.

Amazon API Gateway tracks the number of requests per second. Any requests over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response.

The option that says: API Gateway will automatically scale and handle massive traffic spikes so you do not have to do anything is incorrect because although it can scale using AWS Edge locations, you still need to configure the throttling to further manage the bursts of your APIs.

Manually upgrading the EC2 instances being used by API Gateway is incorrect because API Gateway is a fully managed service and hence, you do not have access to its underlying resources.

Deploying Multi-AZ in API Gateway with Read Replica is incorrect because RDS has Multi-AZ and Read Replica capabilities, and not API Gateway.

Reference:

https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching

[Go back to Q329](#)

Answer to Q330: A, B

[Go back to Q330](#)

Explanation to Q330

By using Versioning and enabling MFA (Multi-Factor Authentication) Delete, you can secure and recover your S3 objects from accidental deletion or overwrite.

Versioning is a means of keeping multiple variants of an object in the same bucket. Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

You can also optionally add another layer of security by configuring a bucket to enable MFA (Multi-Factor Authentication) Delete, which requires additional authentication for either of the following operations:

- Change the versioning state of your bucket

- Permanently delete an object version

MFA Delete requires two forms of authentication together:

- Your security credentials
- The concatenation of a valid serial number, a space, and the six-digit code displayed on an approved authentication device

Providing access to S3 data strictly through pre-signed URL only is incorrect since a pre-signed URL gives access to the object identified in the URL. Pre-signed URLs are useful when customers perform an object upload to your S3 bucket but does not help in preventing accidental deletes.

Disallowing S3 Delete using an IAM bucket policy is incorrect since you still want users to be able to delete objects in the bucket, and you just want to prevent accidental deletions. Disallowing S3 Delete using an IAM bucket policy will restrict all delete operations to your bucket.

Enabling Amazon S3 Intelligent-Tiering is incorrect since S3 intelligent tiering does not help in this situation.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

[Go back to Q330](#)

Answer to Q331: D

[Go back to Q331](#)

[Explanation to Q331](#)

Amazon API Gateway provides throttling at multiple levels including global and by service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs and configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds. Amazon API Gateway tracks the number of requests per second. Any request over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response. Hence, enabling throttling limits and result caching in API Gateway is the correct answer.

You can add caching to API calls by provisioning an Amazon API Gateway cache and specifying its size in gigabytes. The cache is provisioned for a specific stage of your APIs. This improves performance and reduces the traffic sent to your back end. Cache settings allow you to control the way the cache key is built and the time-to-live (TTL) of the data stored for each method. Amazon API Gateway also exposes management APIs that help you invalidate the cache for each stage.

The option that says: Switch from using AWS Lambda and API Gateway to a more scalable and highly available architecture using EC2 instances, ELB, and Auto Scaling is incorrect since there is no need to transfer your applications to other services.

Using CloudFront in front of the API Gateway to act as a cache is incorrect because CloudFront only speeds up content delivery which provides a better latency experience for your users. It does not help much for the backend.

Moving the Lambda function in a VPC is incorrect because this answer is irrelevant to what is being asked. A VPC is your own virtual private cloud where you can launch AWS services.

Reference:

<https://aws.amazon.com/api-gateway/faqs/>

[Go back to Q331](#)

Answer to Q332: D

[Go back to Q332](#)

Explanation to Q332

NA

[Go back to Q332](#)

Answer to Q333: A, B

[Go back to Q333](#)

Explanation to Q333

NA

[Go back to Q333](#)

Answer to Q334: B

[Go back to Q334](#)

Explanation to Q334

NA

[Go back to Q334](#)

Answer to Q335: B

[Go back to Q335](#)

Explanation to Q335

An event in CloudTrail is the record of an activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. There are two types of events that can be logged in CloudTrail: management events and data events. By default, trails log management events, but not data events.

A trail can be applied to all regions or a single region. As a best practice, create a trail that applies to all regions in the AWS partition in which you are working. This is the default setting when you create a trail in the CloudTrail console.

For most services, events are recorded in the region where the action occurred. For global services such as AWS Identity and Access Management (IAM), AWS STS, Amazon CloudFront, and Route 53, events are delivered to any trail that includes global services and are logged as occurring in US East (N. Virginia) Region.

In this scenario, the company requires a secure and durable logging solution that will track all the activities of all AWS resources on all regions. CloudTrail can be used for this case with multi-region trail enabled, however, it will only cover the activities of the regional services (EC2, S3, RDS etc.) and not for global services such as IAM, CloudFront, AWS WAF, and Route 53. In order to satisfy the requirement, you must add the --include-global-service-events parameter in your AWS CLI command.

The option that says: Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and 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 is correct because it provides security, integrity, and durability to your log data and in addition, it has the -include-global-

service-events parameter enabled which will also include activity from global services such as IAM, Route 53, AWS WAF, and CloudFront.

The option that says: Set up a new CloudWatch trail in a new S3 bucket using the AWS CLI and 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 is incorrect because you need to use CloudTrail instead of CloudWatch.

The option that says: Set up a new CloudWatch trail in a new S3 bucket using the CloudTrail console and 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 is incorrect because you need to use CloudTrail instead of CloudWatch. In addition, the --include-global-service-events parameter is also missing in this setup.

The option that says: Set up a new CloudTrail trail in a new S3 bucket using the AWS CLI and 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 is incorrect because the --is-multi-region-trail is not enough as you also need to add the --include-global-service-events parameter and not --no-include-global-service-events. Plus, you cannot enable the Global Service Events using the CloudTrail console but by using AWS CLI.

References:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events>

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail-by-using-the-aws-cli.html>

[Go back to Q335](#)

Answer to Q336: C

[Go back to Q336](#)

Explanation to Q336

The reason for this issue is that IAM users are created with no permissions by default. That means that when you created the new IAM user, you might not provision any permissions to the user.

Hence, the option that says: IAM users are created by default with no permissions is correct and conversely, the options that say: IAM users are created by default with partial permissions and IAM users are created by default with full permissions incorrect.

The option that says: You need to wait for 24 hours for the new IAM user to have access is incorrect because provisions are applied immediately, and not after 24 hours.

The IAM user might need to make API calls or use the AWS CLI or the Tools for Windows PowerShell. In that case, create an access key (an access key ID and a secret access key) for that user. This is called Programmatic access.

If the user needs to access AWS resources from the AWS Management Console, create a password and provide it to the user.

Reference:

<https://aws.amazon.com/iam/details/manage-users/>

[Go back to Q336](#)

Answer to Q337: B

[Go back to Q337](#)

Explanation to Q337

NA

[Go back to Q337](#)

Answer to Q338: B, D

[Go back to Q338](#)

Explanation to Q338

DynamoDB and ElastiCache are the correct answers. You can store session state data on both DynamoDB and ElastiCache. These AWS services provide high-performance storage of key-value pairs which can be used to build a highly available web application.

Redshift Spectrum is incorrect since this is a data warehousing solution where you can directly query data from your data warehouse. Redshift is not suitable for storing session state, but more on analytics and OLAP processes.

RDS is incorrect as well since this is a relational database solution of AWS. This relational storage type might not be the best fit for session states, and it might not provide the performance you need compared to DynamoDB for the same cost. S3 Glacier is incorrect as well since this is a low-cost cloud storage service for data archiving and long-term backup. The archival and retrieval speeds of Glacier is too slow for handling session states.

References:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/caching/session-management/>

[Go back to Q338](#)

Answer to Q339: A, D

[Go back to Q339](#)

Explanation to Q339

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. Because of this, storing data in S3 One Zone-IA costs 20% less than storing it in S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA storage.

It's a good choice, for example, for storing secondary backup copies of on-premises data or easily re-creatable data, or for storage used as an S3 Cross-Region Replication target from another AWS Region. S3 One Zone-IA offers the same high durability, high throughput, and low latency of Amazon S3 Standard and S3 Standard-IA, with a low per GB storage price and per GB retrieval fee. The S3 One Zone-IA storage class is set at the object level and can exist in the same bucket as S3 Standard and S3 Standard-IA, allowing you to use S3 Lifecycle Policies to automatically transition objects between storage classes without any application changes.

Key Features:

- Same low latency and high throughput performance of S3 Standard and S3 Standard-IA
- Designed for durability of 99.99999999% of objects in a single Availability Zone, but data will be lost in the event of Availability Zone destruction
- Designed for 99.5% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest
- Lifecycle management for automatic migration of objects

Remember that since the S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.

Reference :

https://aws.amazon.com/s3/storage-classes/#Amazon_S3_One_Zone-Infrequent_Access

[Go back to Q339](#)

Answer to Q340: C

[Go back to Q340](#)

Explanation to Q340

CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content. If you want to serve private content through CloudFront and you're trying to decide whether to use signed URLs or signed cookies.

Use signed URLs for the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions
- You want to restrict access to individual files, for example, an installation download for your application
- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies

Use signed cookies for the following cases:

- You want to provide access to multiple restricted files, for example, all the files for a video in HLS format or all the files in the subscribers' area of a website
- You don't want to change your current URLs

Hence, the correct answer for this scenario is the option that says: 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.

The option that says: 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 is incorrect because a Match Viewer is an Origin Protocol Policy which configures CloudFront to communicate with your origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

The option that says: Create a Signed URL with a custom policy which only allows the members to see the private files is incorrect because Signed URLs are primarily used for providing access to individual files, as shown on the above explanation. In addition, the scenario explicitly says that they don't want to change their current URLs which is why implementing Signed Cookies is more suitable than Signed URL.

The option that says: Configure your CloudFront distribution to use Field-Level Encryption to protect your private data and only allow access to members is incorrect because Field-Level Encryption only allows you to securely upload user-submitted sensitive information to your web servers. It does not provide access to download multiple private files.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

[Go back to Q340](#)

Answer to Q341: A

[Go back to Q341](#)

Explanation to Q341

When you create or update Lambda functions that use environment variables, AWS Lambda encrypts them using the AWS Key Management Service. When your Lambda function is invoked, those values are decrypted and made available to the Lambda code.

The first time you create or update Lambda functions that use environment variables in a region, a default service key is created for you automatically within AWS KMS. This key is used to encrypt environment variables.

However, if you wish to use encryption helpers and use KMS to encrypt environment variables after your Lambda function is created, you must create your own AWS KMS key and choose it instead of the default key. The default key will give errors when chosen. Creating your own key gives you more flexibility, including the ability to create, rotate, disable, and define access controls, and to audit the encryption keys used to protect your data.

The option that says: There is no need to do anything because, by default, AWS Lambda already encrypts the environment variables using the AWS Key Management Service is incorrect because although Lambda encrypts the environment variables in your function by default, the sensitive information would still be visible to other users who have access to the Lambda console. This is because Lambda uses a default KMS key to encrypt the variables, which is usually accessible by other users.

The best option in this scenario is to use encryption helpers to secure your environment variables.

The option that says: Enable SSL encryption that leverages on AWS CloudHSM to store and encrypt the sensitive information is also incorrect since enabling SSL would encrypt data only when in-transit. Your other teams would still be able to view the plaintext at-rest. Use AWS KMS instead.

The option that says: AWS Lambda does not provide encryption for the environment variables. Deploy your code to an EC2 instance instead is incorrect since, as mentioned, Lambda does provide encryption functionality of environment variables.

References:

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html#env_encrypt

https://docs.aws.amazon.com/lambda/latest/dg/tutorial-env_console.html

[Go back to Q341](#)

Answer to Q342: A

[Go back to Q342](#)

Explanation to Q342

In an ideal and secure VPC architecture, you launch the web servers or elastic load balancers in the public subnet and the database servers in the private subnet.

The private subnet is correct because it is more secure to launch your database in the private subnet to prevent other external and unauthorized users to access or attack your system.

The public subnet is incorrect because if you launch your database server in the public subnet, it will be publicly accessible all over the Internet which has a higher security risk.

Either public or private subnet is incorrect since only the private subnet is the correct answer if you want to secure your database from external traffic.

The option that says: Ideally be launched outside the Amazon VPC is incorrect as there is no need to launch it outside the VPC. Having it run in a private subnet should address the security and networking concerns of your database.

Reference:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

[Go back to Q342](#)

Answer to Q343: C

[Go back to Q343](#)

Explanation to Q343

NA

[Go back to Q343](#)

Answer to Q344: D

[Go back to Q344](#)

Explanation to Q344

The word ephemeral means "short-lived" or "temporary" in the English dictionary. Hence, when you see this word in AWS, always consider this as just a temporary memory or a short-lived storage.

The virtual devices for instance store volumes are named as ephemeral[0-23]. Instance types that support one instance store volume have ephemeral0. Instance types that support two instance store volumes have ephemeral0 and ephemeral1, and so on until ephemeral23. The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists.

However, data in the instance store is lost under the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

Hence, the option that says: Data will be deleted is the correct answer.

The option that says: Data is automatically saved in an EBS volume is incorrect since instance store volumes and EBS volumes are two different storage types. An Amazon EBS volume is a durable, block-level storage device that you can attach to a single EC2 instance. An instance store provides temporary block-level storage and is located on disks that are physically attached to the host computer. No automatic backup will be performed.

The option that says: Data is unavailable until the instance is restarted is incorrect because once you stop an instance, the data in the ephemeral instance store volumes will be gone.

The option that says: Data is automatically saved as an EBS snapshot is incorrect because just like in the option above, instance store volumes and EBS volumes are two different storage devices. There is no automated snapshot that will be created.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html?shortFooter=true#instance-store-lifetime>

[Go back to Q344](#)

Answer to Q345: C, D

[Go back to Q345](#)

Explanation to Q345

NA

[Go back to Q345](#)

Answer to Q346: C

[Go back to Q346](#)

Explanation to Q346

Amazon MQ, Amazon SQS, and Amazon SNS are messaging services that are suitable for anyone from startups to enterprises. If you're using messaging with existing applications and want to move your messaging service to the cloud quickly and easily, it is recommended that you consider Amazon MQ. It supports industry-standard APIs and protocols so you can switch from any standards-based message broker to Amazon MQ without rewriting the messaging code in your applications.

Hence, Amazon MQ is the correct answer.

If you are building brand new applications in the cloud, then it is highly recommended that you consider Amazon SQS and Amazon SNS. Amazon SQS and SNS are lightweight, fully managed message queue and topic services that scale almost infinitely and provide simple, easy-to-use APIs. You can use Amazon SQS and SNS to decouple and scale microservices, distributed systems, and serverless applications, and improve reliability.

Amazon SQS is incorrect because although this is a fully managed message queuing service, it does not support an extensive list of industry-standard messaging APIs and protocol, unlike Amazon MQ. Moreover, using Amazon SQS requires you to do additional changes in the messaging code of applications to make it compatible.

Amazon SNS is incorrect because SNS is more suitable as a pub/sub messaging service instead of a message broker service.

Amazon SWF is incorrect because this is a fully-managed state tracker and task coordinator service and not a messaging service, unlike Amazon MQ, AmazonSQS and Amazon SNS.

References:

<https://aws.amazon.com/amazon-mq/faqs/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sqsdifferencefromamazonmqsns>

[Go back to Q346](#) +

Answer to Q347: A

[Go back to Q347](#)

Explanation to Q347

To avoid accidental deletion in Amazon S3 bucket, you can:

- Enable Versioning
- Enable MFA (Multi-Factor Authentication) Delete

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.

With versioning, you can easily recover from both unintended user actions and application failures.

If the MFA (Multi-Factor Authentication) Delete is enabled, it requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

Using S3 Infrequently Accessed storage to store the data is incorrect. Switching your storage class to S3 Infrequent Access won't help mitigate accidental deletions.

Setting up a signed URL for all users is incorrect. Signed URLs give you more control over access to your content, so this feature deals more on accessing rather than deletion.

Creating an IAM bucket policy that disables delete operation is incorrect. If you create a bucket policy preventing deletion, other users won't be able to delete objects that should be deleted. You only want to prevent accidental deletion, not disable the action itself.

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

[Go back to Q347](#)

Answer to Q348: A

[Go back to Q348](#)

Explanation to Q348

Transferring data from an EC2 instance to Amazon S3, Amazon Glacier, Amazon DynamoDB, Amazon SES, Amazon SQS, or Amazon SimpleDB in the same AWS Region has no cost at all. Refer to the Amazon EC2 Pricing on the link below for reference.

The options that say: You are only using an On-Demand EC2 instance which is exactly the same price as Spot EC2 instance, launched by a persistent Spot request and You are only using an On-Demand EC2 instance so the cost will be lower than a Spot instance are incorrect since an On-Demand instance costs more than a Spot instance.

The option that says: Transferring data from an EC2 instance to an S3 bucket in the same region has a 50% discount based on the AWS Pricing is incorrect as there is no such thing as 50% discount when transferring data from an EC2 instance to an S3 bucket in the same region.

Reference:

https://aws.amazon.com/ec2/pricing/on-demand/#Data_Transfer

[Go back to Q348](#)

Answer to Q349: A, D

[Go back to Q349](#)

Explanation to Q349

The goal here is to increase the write performance of the database hosted in an EC2 instance. You can achieve this by either setting up a standard RAID 0 configuration or simply by increasing the size of the EC2 instance.

Some EC2 instance types can drive more I/O throughput than what you can provision for a single EBS volume. You can join multiple gp2, io1, st1, or sc1 volumes together in a RAID 0 configuration to use the available bandwidth for these instances.

With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, if that RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.

Take note that HVM AMIs are required to take advantage of enhanced networking and GPU processing.

In order to pass through instructions to specialized network and GPU devices, the OS needs to be able to have access to the native hardware platform which the HVM virtualization provides.

Re-launching the instance with a Paravirtual (PV) AMI and enabling Enhanced Networking is incorrect because although the Enhanced Networking feature can provide higher I/O performance and lower CPU utilization to your EC2 instance, you must use an HVM AMI instead of PV AMI.

Using a standard RAID 1 configuration with two EBS Volumes is incorrect because the main use case for RAID 1 is to provide mirroring, redundancy, and fault-tolerance. RAID 0 is a more suitable option for providing faster read and write operations, compared with RAID 1.

Setting up the EC2 instance in a placement group is incorrect because the placement groups feature is primarily used for inter-instance communication.

References :

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSPerformance.html>

<https://aws.amazon.com/ec2/features/#enhanced-networking>

[Go back to Q349](#)

Answer to Q350: A

[Go back to Q350](#)

Explanation to Q350

Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.

To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action. At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

Hence, configuring a Scheduled scaling policy for the Auto Scaling group to launch new instances before the start of the day is the correct answer. You need to configure a Scheduled scaling policy. This will ensure that the instances are already scaled up and ready before the start of the day since this is when the application is used the most.

Configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the CPU utilization and configuring a Dynamic scaling policy for the Auto Scaling group to launch new instances based on the Memory utilization are both incorrect because although these are valid solutions, it is still better to configure a Scheduled scaling policy as you already know the exact peak hours of your application. By the time either the CPU or Memory hits a peak, the application already has performance issues, so you need to ensure the scaling is done beforehand using a Scheduled scaling policy.

Setting up an Application Load Balancer (ALB) to your architecture to ensure that the traffic is properly distributed on the instances is incorrect.

Although the Application load balancer can also balance the traffic, it cannot increase the instances based on demand.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

[Go back to Q350](#)

Answer to Q351: A

[Go back to Q351](#)

Explanation to Q351

NA

[Go back to Q351](#)

Answer to Q352: D

[Go back to Q352](#)

Explanation to Q352

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

DynamoDB is incorrect because this is primarily used as a NoSQL database which supports both document and key-value store models. ElastiCache is a more suitable service to use than DynamoDB, if you need an in-memory data store.

Amazon RDS is incorrect because this is mainly used as a relational database and not as a data storage for frequently used data.

Amazon Redshift is incorrect because this is a data warehouse service and is not suitable to be used as an in-memory data store.

References:

<https://aws.amazon.com/elasticache/>
<https://aws.amazon.com/products/databases/>

[Go back to Q352](#)

Answer to Q353: C

[Go back to Q353](#)

Explanation to Q353

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

Budgets can be tracked at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic.

You can also use AWS Budgets to set a custom reservation utilization target and receive alerts when your utilization drops below the threshold you define. RI utilization alerts support Amazon EC2, Amazon RDS, Amazon Redshift, and Amazon ElastiCache reservations.

Budgets can be created and tracked from the AWS Budgets dashboard or via the Budgets API.

Cost Explorer is incorrect because it only helps you visualize and manage your AWS costs and usages over time. It offers a set of reports you can view data with for up to the last 13 months, forecast how much you're likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase. You use Cost Explorer to identify areas that need further inquiry and see trends to understand your costs.

Cost Allocation Tags is incorrect because it only eases the organization of your resource costs on your cost allocation report to make it easier for you to categorize and track your AWS costs.

Payment History is incorrect because this option only provides a location where you can view the monthly invoices you receive from AWS. If your account isn't past due, the Payment History page shows only previous invoices and payment status.

Reference:

<https://aws.amazon.com/aws-cost-management/aws-budgets/>

[Go back to Q353](#)

Answer to Q354: B

[Go back to Q354](#)

Explanation to Q354

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, API calls, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

CloudWatch is incorrect because although this is also a monitoring service, it cannot track the API calls to your AWS resources.

AWS X-Ray is incorrect because this is not a suitable service to use to track each API call to your AWS resources. It just helps you debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance.

Redshift Spectrum is incorrect because this is not a monitoring service but rather a feature of Amazon Redshift that enables you to query and analyze all of your data in Amazon S3 using the open data formats you already use, with no data loading or transformations needed.

Reference:

<https://aws.amazon.com/cloudtrail/>

[Go back to Q354](#)

Answer to Q355: C

[Go back to Q355](#)

Explanation to Q355

In Amazon S3, all objects are private by default. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a pre-signed URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The pre-signed URLs are valid only for the specified duration.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

Using CloudFront distributions for your photos is incorrect. CloudFront is a content delivery network service that speeds up delivery of content to your customers.

Blocking the IP addresses of the offending websites using NACL is also incorrect. Blocking IP address using NACLs is not a very efficient method because a quick change in IP address would easily bypass this configuration.

Storing photos on an Amazon EBS volume of the web server is also incorrect. You cannot serve objects directly from an EBS volume, which needs to be attached to an EC2 instance. EBS volumes also do not provide the same durability as compared to S3.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

[Go back to Q355](#)

Answer to Q356: D

[Go back to Q356](#)

[Explanation to Q356](#)

When you create or modify your DB instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB instance failure.

RDS Read Replica is incorrect as a Read Replica provides an asynchronous replication instead of synchronous.

DynamoDB Read Replica and CloudFront running as a Multi-AZ deployment are incorrect as both DynamoDB and CloudFront do not have a Read Replica feature.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q356](#)

Answer to Q357: C

[Go back to Q357](#)

Explanation to Q357

On a given volume configuration, certain I/O characteristics drive the performance behavior for your EBS volumes. SSD-backed volumes, such as General Purpose SSD (gp2) and Provisioned IOPS SSD (io1), deliver consistent performance whether an I/O operation is random or sequential. HDD-backed volumes like Throughput Optimized HDD (st1) and Cold HDD (sc1) deliver optimal performance only when I/O operations are large and sequential.

In the exam, always consider the difference between SSD and HDD as shown on the table below. This will allow you to easily eliminate specific EBS-types in the options which are not SSD or not HDD, depending on whether the question asks for a storage type which has small, random I/O operations or large, sequential I/O operations.

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.

General Purpose SSD (gp2) is incorrect because although General Purpose is a type of SSD that can handle small, random I/O operations, the Provisioned IOPS SSD volumes are much more suitable to meet the needs of I/O-intensive database workloads such as MongoDB, Oracle, MySQL, and many others.

Throughput Optimized HDD (st1) and Cold HDD (sc1) are incorrect because HDD volumes (such as Throughput Optimized HDD and Cold HDD volumes) are more suitable for workloads with large, sequential I/O operations instead of small, random I/O operations.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeType.html#EBSVolumeTypes_piops

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html>

[Go back to Q357](#)

Answer to Q358: B

[Go back to Q358](#)

Explanation to Q358

The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly. With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.
2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.
3. If there are multiple instances to terminate based on the above criteria, determine which unprotected instances are closest to the next billing hour. (This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.
4. If there is more than one unprotected instance closest to the next billing hour, choose one of these instances at random.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-termination-policy>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>

[Go back to Q358](#)

Answer to Q359: C

[Go back to Q359](#)

Explanation to Q359

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. For this scenario, enabling Multi-AZ failover is the correct answer. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.

Making a snapshot of the database allows you to have a backup of your database, but it does not provide immediate availability in case of AZ failure. So, this is incorrect.

Increasing the database instance size is not a solution for this problem. Doing this action addresses the need to upgrade your compute capacity but does not solve the requirement of providing access to your database even in the event of a loss of one of the Availability Zones.

Creating a read replica is incorrect because this simply provides enhanced performance for read-heavy database workloads. Although you can promote a read replica, its asynchronous replication might not provide you the latest version of your database.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q359](#)

Answer to Q360: A

[Go back to Q360](#)

Explanation to Q360

To calculate the total number of IP addresses of a given CIDR Block, you simply need to follow the 2 easy steps below. Let's say you have a CIDR block /27:1. Subtract 32 with the mask number : $(32 - 27) = 5$. Raise the number 2 to the power of the answer in Step #1 : $2^5 = (2 * 2 * 2 * 2 * 2) = 32$ The answer to Step #2 is the total number of IP addresses available in the given CIDR netmask. Don't forget that in AWS, the first 4 IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance. In addition, you can always associate a netmask of /27 which also has the same number of usable IP addresses (27) to help you with your exam.

The correct answer is 172.0.0.0/27 because the CIDR block of 172.0.0.0/27, with a netmask of /27, has an equivalent of 27 usable IP addresses. Take note that a netmask of /27 originally provides you with 32 IP addresses but in AWS, there are 5 IP addresses that are reserved which you cannot use. The first 4 IP addresses and the last IP address in each subnet CIDR block are not available in your VPC which means that you have to always subtract 5 IP addresses, hence $32 - 5 = 27$.This option is incorrect: 172.0.0.0/28 as a netmask of /28 only supports 16 IP Addresses.

The following options are also incorrect: 172.0.0.0/29 and 172.0.0.0/30 as the only allowed block size is between a /28 netmask and /16 netmask.

To add a CIDR block to your VPC, the following rules apply:

1. The allowed block size is between a /28 netmask and /16 netmask.
2. The CIDR block must not overlap with any existing CIDR block that's associated with the VPC. You cannot increase or decrease the size of an existing CIDR block.
3. You have a limit on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your limits.
4. The CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables. For example, if you have a route with a destination of 10.0.0.0/24 to a virtual private gateway, you cannot associate a CIDR block of the same range or larger.

However, you can associate a CIDR block of 10.0.0.0/25 or smaller.

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

[Go back to Q360](#)

Answer to Q361: D

[Go back to Q361](#)

Explanation to Q361

Amazon Aurora typically involves a cluster of DB instances instead of a single instance. Each connection is handled by a specific DB instance. When

you connect to an Aurora cluster, the host name and port that you specify point to an intermediate handler called an endpoint. Aurora uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the hostnames or write your own logic for load-balancing and rerouting connections when some DB instances aren't available.

For certain Aurora tasks, different instances or groups of instances perform different roles. For example, the primary instance handles all data definition language (DDL) and data manipulation language (DML) statements. Up to 15 Aurora Replicas handle read-only query traffic.

Using endpoints, you can map each connection to the appropriate instance or group of instances based on your use case. For example, to perform DDL statements you can connect to whichever instance is the primary instance. To perform queries, you can connect to the reader endpoint, with Aurora automatically performing load-balancing among all the Aurora Replicas. For clusters with DB instances of different capacities or configurations, you can connect to custom endpoints associated with different subsets of DB instances. For diagnosis or tuning, you can connect to a specific instance endpoint to examine details about a specific DB instance.

The custom endpoint provides load-balanced database connections based on criteria other than the read-only or read-write capability of the DB instances. For example, you might define a custom endpoint to connect to instances that use a AWS instance class or a particular DB parameter group. Then you might tell groups of users about this custom endpoint. For example, you might direct internal users to low-capacity instances for report generation or ad hoc (one-time) querying, and direct production traffic to high-capacity instances. Hence, creating a custom endpoint in Aurora based on the specified criteria for the production traffic and another custom endpoint to handle the reporting queries is the correct answer.

Configuring 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 is incorrect because although it is true that a reader endpoint enables your Aurora database to automatically perform load-balancing among all the Aurora Replicas, it is quite limited to doing read operations only. You still need to use a custom endpoint to load-balance the database connections based on the specified criteria.

The option that says: 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 is incorrect because a cluster endpoint (also known as a writer endpoint) for an Aurora DB cluster simply connects to the current primary DB instance for that DB cluster. This endpoint can perform write operations in the database such as DDL statements, which is perfect for handling production traffic but not suitable for handling queries for reporting since there will be no write database operations that will be sent. Moreover, the endpoint does not point to lower-capacity or high-capacity instances as per the requirement. A better solution for this is to use a custom endpoint.

The option that says: 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 is incorrect because Aurora does not do this by default. You must create custom endpoints in order to accomplish this requirement.

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html>

[Go back to Q361](#)

Answer to Q362: D

[Go back to Q362](#)

Explanation to Q362

In case that one of the EC2 instances failed a health check, the Application Load Balancer stops sending traffic to that instance.

Your Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target group with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

Reference:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

[Go back to Q362](#)

Answer to Q363: A

[Go back to Q363](#)

Explanation to Q363

Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing applications and tools. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide

a common data source for workloads and applications running on more than one Amazon EC2 instance.

This scenario tests your understanding of EBS, EFS, and S3. In this scenario, there is a fleet of On-Demand EC2 instances that stores file documents from the users to one of the attached EBS Volumes. The system performance is quite slow because the architecture doesn't provide the EC2 instances a parallel shared access to the file documents.

Remember that an EBS Volume can be attached to one EC2 instance at a time, hence, no other EC2 instance can connect to that EBS Provisioned IOPS Volume. Take note as well that the type of storage needed here is a "file storage" which means that S3 is not the best service to use because it is mainly used for "object storage", and S3 does not provide the notion of "folders" too. Therefore, using EFS is the correct answer.

Upgrading your existing EBS volumes to Provisioned IOPS SSD Volumes is incorrect because the scenario requires you to set up a scalable, high throughput storage system that will allow concurrent access from multiple EC2 instances. This is clearly not possible in EBS, even with Provisioned IOPS SSD Volumes. You must use EFS instead.

Using ElastiCache is incorrect because this is an in-memory data store that improves the performance of your applications, which is not what you need since it is not a file storage.

Reference:

<https://aws.amazon.com/efs/>

[Go back to Q363](#)

Answer to Q364: C

[Go back to Q364](#)

Explanation to Q364

In this scenario, the load balancer will route the incoming requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.

There are two ways of checking the status of your EC2 instances:

1. Via the Auto Scaling group
2. Via the ELB health checks

The default health checks for an Auto Scaling group are EC2 status checks only. If an instance fails these status checks, the Auto Scaling group considers the instance unhealthy and replaces. If you attached one or more load balancers or target groups to your Auto Scaling group, the group does not, by default, consider an instance unhealthy and replace it if it fails the load balancer health checks.

However, you can optionally configure the Auto Scaling group to use Elastic Load Balancing health checks. This ensures that the group can determine an instance's health based on additional tests provided by the load balancer. The load balancer periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. If you configure the Auto Scaling group to use Elastic Load Balancing health checks, it considers the instance unhealthy if it fails either the EC2 status checks or the load balancer health checks. If you attach multiple load balancers to an Auto Scaling group, all of them must report that the instance is healthy for it to consider the instance healthy. If one load balancer reports an instance as unhealthy, the Auto Scaling group replaces the instance, even if other load balancers report it as healthy. The scenario said that the Auto Scaling group is configured with default settings. This means that it is using the EC2 health check type. Hence, the correct answer is: The ELB stops sending traffic to the EC2 instance.

The option that says: The EC2 instance gets terminated automatically by the ELB is incorrect because this action will not be done by ELB.

The option that says: The EC2 instance will automatically be deregistered from the default Placement Group is incorrect because in the first place, an EC2 instance is not associated with a Placement Group by default. A Placement group is simply a logical placement of a group of interdependent EC2 instances to meet the low-latency network performance needs of your workload.

The option that says: The EC2 instance is replaced automatically by the ELB is incorrect because the scenario clearly states that the Auto Scaling group is configured with default settings. The default health check type is the EC2 checks, which means that the ELB will stop sending traffic to the EC2 instance.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html>

[Go back to Q364](#)

Answer to Q365: A, D

[Go back to Q365](#)

Explanation to Q365

NA

[Go back to Q365](#)

Answer to Q366: B

[Go back to Q366](#)

Explanation to Q366

A DynamoDB stream is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

Whenever an application creates, updates, or deletes items in the table, DynamoDB Streams writes a stream record with the primary key attribute(s) of the items that were modified. A stream record contains information about a data modification to a single item in a DynamoDB table. You can configure the stream so that the stream records capture additional information, such as the "before" and "after" images of modified items.

Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers, pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.

If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records. The Lambda function can perform any actions you specify, such as sending a notification or initiating a workflow.

Hence, the correct answer in this scenario is the option that says: Enable DynamoDB Stream and create an AWS Lambda trigger, as well as the IAM role which contains all 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.

The option that says: 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 user, notify the subscribers via email using SNS is incorrect because although this is a valid solution, it is missing a vital step which is to enable DynamoDB Streams. With the DynamoDB Streams Kinesis Adapter in place, you can begin developing applications via the KCL interface, with the API calls seamlessly directed at the DynamoDB Streams endpoint. Remember that the DynamoDB Stream feature is not enabled by default.

The option that says: 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 is incorrect because just like in the above, you have to manually enable DynamoDB Streams first before you can use its endpoint.

The option that says: 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 is incorrect because the DynamoDB Accelerator (DAX) feature is primarily used to significantly improve the in-memory read performance of your database, and not to capture the time-ordered sequence of item-level modifications. You should use DynamoDB Streams in this scenario instead.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.Tutorial.html>

[Go back to Q366](#)

Answer to Q367: A, D

[Go back to Q367](#)

Explanation to Q367

Reserved Instances (RIs) provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefiting from RI pricing when you use Convertible RIs. One important thing to remember here is that Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account.

When your computing needs change, you can modify your Standard or Convertible Reserved Instances and continue to take advantage of the billing benefit. You can modify the Availability Zone, scope, network platform, or instance size (within the same instance type) of your Reserved Instance. You can also sell your unused instance on the Reserved Instance Marketplace.

The option that says: Reserved Instances don't get interrupted unlike Spot instances if there are not enough unused EC2 instances to meet the demand is correct.

Likewise, the option that says: You can have capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term through Scheduled Reserved Instances is correct. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

The option that says: Standard Reserved Instances can be later exchanged for other Convertible Reserved Instances is incorrect because only

Convertible Reserved Instances can be exchanged for other Convertible Reserved Instances.

The option that says: It can enable you to reserve capacity for your Amazon EC2 instances in multiple Availability Zones and multiple AWS Regions for any duration is incorrect because you can reserve capacity to a specific AWS Region (regional Reserved Instance) or specific Availability Zone (zonal Reserved Instance) only. You cannot reserve capacity to multiple AWS Regions in a single RI purchase.

The option that says: It runs in a VPC on hardware that's dedicated to a single customer is incorrect because that is the description of a Dedicated instance and not a Reserved Instance. A Dedicated instance runs in a VPC on hardware that's dedicated to a single customer.

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-modifying.html>

<https://aws.amazon.com/ec2/pricing/reserved-instances/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html>

[Go back to Q367](#)

Answer to Q368: B, E

[Go back to Q368](#)

[Explanation to Q368](#)

The question refers to one of the common scenarios for temporary credentials in AWS. Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles. In this example, it is called enterprise identity federation considering that you also need to set up a single sign-on (SSO) capability.

The correct answers are:- Setup a Federation proxy or an Identity provider- Setup an AWS Security Token Service to generate temporary tokens- Configure an IAM role and an IAM Policy to access the bucket.

In an enterprise identity federation, you can authenticate users in your organization's network, and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate username and password. This is known as the single sign-on (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory. You can also use SAML 2.0 to manage your own solution for federating user identities.

Using 3rd party Single Sign-On solutions such as Atlassian Crowd, OKTA, OneLogin and many others is incorrect since you don't have to use 3rd party solutions to provide the access. AWS already provides the necessary tools that you can use in this situation.

Using a resource tag on each folder in the S3 bucket is incorrect since doing this won't help restrict access to a specific user.

Setting up a matching IAM user for each 1200 users in your corporate directory that needs access to a folder in the S3 bucket is incorrect since creating that many IAM users would be unnecessary. Also, you want the account to integrate with your AD or LDAP directory, hence, IAM Users does not fit these criteria.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_section.html

[Go back to Q368](#)

Answer to Q369: C

[Go back to Q369](#)

Explanation to Q369

To control the traffic coming in and out of your VPC network, you can use the network access control list (ACL). It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. This is the best solution among other options as you can easily add and remove the restriction in a matter of minutes.

Creating a policy in IAM to deny access from the IP Address block is incorrect as an IAM policy does not control the inbound and outbound traffic of your VPC.

Adding a rule in the Security Group of the EC2 instances to deny access from the IP Address block is incorrect as although a Security Group acts as a firewall, it will only control both inbound and outbound traffic at the instance level and not on the whole VPC.

Configuring the firewall in the operating system of the EC2 instances to deny access from the IP address block is incorrect because adding a firewall in the underlying operating system of the EC2 instance is not enough; the attacker can just connect to other AWS resources since the network access control list still allows them to do so.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[Go back to Q369](#)

Answer to Q370: A

[Go back to Q370](#)

Explanation to Q370

To achieve this requirement, you can deploy your Oracle database to Amazon EC2 instances with data replication between two different Availability Zones.

Hence, option A is the correct answer. The deployment of this architecture can easily be achieved by using CloudFormation and Quick Start. Please refer to the reference link for information.

The Quick Start deploys the Oracle primary database (using the preconfigured, general-purpose starter database from Oracle) on an Amazon EC2 instance in the first Availability Zone. It then sets up a second EC2 instance in a second Availability Zone, copies the primary database to the second instance by using the DUPLICATE command, and configures Oracle Data Guard.

Amazon RDS and Amazon RDS with Multi-AZ deployments are both incorrect because the scenario requires you to have access to the underlying operating system of the database server. Remember that Amazon RDS is a managed database service, which means that Amazon is the one that manages the underlying operating system of the database instance and not you.

The option that says: Amazon EC2 instances with data replication in one Availability Zone is incorrect since deploying to just one Availability Zone

(AZ) will not make the database tier highly available. If that AZ went down, your database will be unavailable.

References:

<https://aws.amazon.com/quickstart/>

<https://docs.aws.amazon.com/quickstart/latest/oracle-database/architecture.html>

http://docs.aws.amazon.com/dms/latest/userguide/CHAP_Introduction.ReplicationInstance.html

[Go back to Q370](#)

Answer to Q371: D

[Go back to Q371](#)

Explanation to Q371

NA

[Go back to Q371](#)

Answer to Q372: B

[Go back to Q372](#)

Explanation to Q372

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing(ELB), Amazon CloudFront, and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and

transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.

AWS Shield Advanced also gives you 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing(ELB), Amazon CloudFront, and Amazon Route 53 charges.

The option that says: Using the AWS Firewall Manager, set up a security layer that will prevent SYN floods, UDP reflection attacks and other DDoS attacks is incorrect because the AWS Firewall Manager is mainly used to simplify your AWS WAF administration and maintenance tasks across multiple accounts and resources. It does not protect your VPC against DDoS attacks.

The option that says: Set up a web application firewall using AWS WAF to filter, monitor, and block HTTP traffic is incorrect because even though AWS WAF can help you block common attack patterns to your VPC such as SQL injection or cross-site scripting, this is still not enough to withstand DDoS attacks. It is better to use AWS Shield in this scenario.

The option that says: A combination of Security Groups and Network Access Control Lists to only allow authorized traffic to access your VPC is incorrect because although using a combination of Security Groups and NACLs are valid to provide security to your VPC, this is not enough to mitigate a DDoS attack. You should use AWS Shield for better security protection.

References:

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

<https://aws.amazon.com/shield/>

[Go back to Q372](#)

Answer to Q373: C

[Go back to Q373](#)

Explanation to Q373

CloudWatch has available Amazon EC2 Metrics for you to use for monitoring. CPU Utilization identifies the processing power required to run an application upon a selected instance. Network Utilization identifies the volume of incoming and outgoing network traffic to a single instance. Disk Reads metric is used to determine the volume of the data the application reads from the hard disk of the instance. This can be used to determine the speed of the application. However, there are certain metrics that are not readily available in CloudWatch such as memory utilization, disk space utilization, and many others which can be collected by setting up a custom metric.

You need to prepare a custom metric using CloudWatch Monitoring Scripts which is written in Perl. You can also install CloudWatch Agent to collect more system-level metrics from Amazon EC2 instances. Here's the list of custom metrics that you can set up:

- Memory utilization
- Disk swap utilization
- Disk space utilization
- Page file utilization
- Log collection

CPU Utilization of an EC2 instance, Disk Reads activity of an EC2 instance, and Network packets out of an EC2 instance are all incorrect because these metrics are readily available in CloudWatch by default.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

[Go back to Q373](#)

Answer to Q374: B

[Go back to Q374](#)

Explanation to Q374

NA

[Go back to Q374](#)

Answer to Q375: B

[Go back to Q375](#)

Explanation to Q375

Always remember that the messages in the SQS queue will continue to exist even after the EC2 instance has processed it, until you delete that message. You must ensure that you delete the message after processing to prevent the message from being received and processed again once the visibility timeout expires.

There are three main parts in a distributed messaging system:1. The components of your distributed system (EC2 instances)2. Your queue (distributed on Amazon SQS servers)3. Messages in the queue.

You can set up a system which has several components that send messages to the queue and receive messages from the queue. The queue

redundantly stores the messages across multiple Amazon SQS servers.

Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly.

When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned. While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout.

Component 2 deletes Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

The option that says: The web application is set for long polling so the messages are being sent twice is incorrect because long polling helps reduce the cost of using SQS by eliminating the number of empty responses (when there are no messages available for a `ReceiveMessage` request) and false empty responses (when messages are available but aren't included in a response). Messages being sent twice in an SQS queue configured with long polling is quite unlikely.

The option that says: The web application is set to short polling, so some messages are not being picked up is incorrect since you are receiving emails from SNS where messages are certainly being processed. Following the scenario, messages not being picked up won't result into 20 messages being sent to your inbox.

The option that says: The web application does not have permission to consume messages in the SQS queue is incorrect because not having the correct permissions would have resulted in a different response. The scenario says that messages were properly processed but there were over 20 messages that were sent, hence, there is no problem with the accessing the queue.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html>

[Go back to Q375](#)

Answer to Q376: B

[Go back to Q376](#)

[Explanation to Q376](#)

The partition key portion of a table's primary key determines the logical partitions in which a table's data is stored. This in turn affects the underlying physical partitions. Provisioned I/O capacity for the table is divided evenly among these physical partitions. Therefore, a partition key design that doesn't distribute I/O requests evenly can create "hot" partitions that result in throttling and use your provisioned I/O capacity inefficiently.

The optimal usage of a table's provisioned throughput depends not only on the workload patterns of individual items, but also on the partition-key design. This doesn't mean that you must access all partition key values to achieve an efficient throughput level, or even that the percentage of accessed partition key values must be high. It does mean that the more distinct partition key values that your workload accesses, the more those requests will be spread across the partitioned space. In general, you will use your provisioned throughput more efficiently as the ratio of partition key values accessed to the total number of partition key values increases.

One example for this is the use of partition keys with high-cardinality attributes, which have many distinct values for each item.

Reducing the number of partition keys in the DynamoDB table is incorrect because instead of doing this, you should add more to improve its performance to distribute the I/O requests evenly and not avoid "hot" partitions.

Using partition keys with low-cardinality attributes, which have a few numbers of distinct values for each item is incorrect because this is the exact opposite of the correct answer. Remember that the more distinct partition key values your workload accesses, the more those requests will be spread across the partitioned space. Conversely, the less distinct partition key values, the less evenly spread it would be across the partitioned space, which effectively slows the performance.

The option that says: Avoid using a composite primary key, which is composed of a partition key and a sort key is incorrect because as mentioned, a composite primary key will provide more partition for the table and in turn, improves the performance. Hence, it should be used and not avoided.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-uniform-load.html>

<https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/>

[Go back to Q376](#)

Answer to Q377: B

[Go back to Q377](#)

[**Explanation to Q377**](#)

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console or consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. By default, Enhanced Monitoring metrics are stored in the CloudWatch Logs for 30 days. To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the CloudWatch console.

Take note that there are certain differences between CloudWatch and Enhanced Monitoring Metrics. CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. Hence, enabling Enhanced Monitoring in RDS is the correct answer in this specific scenario.

The differences can be greater if your DB instances use smaller instance classes, because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Using Amazon CloudWatch to monitor the CPU Utilization of your database is incorrect because although you can use this to monitor the CPU Utilization of your database instance, it does not provide the percentage of the CPU bandwidth and total memory consumed by each database process in your RDS instance. Take note that CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance while RDS Enhanced Monitoring gathers its metrics from an agent on the instance.

The option that says: 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 is incorrect because although you can use Amazon CloudWatch Logs and CloudWatch dashboard to monitor the CPU Utilization of the

database instance, using CloudWatch alone is still not enough to get the specific percentage of the CPU bandwidth and total memory consumed by each database processes. The data provided by CloudWatch is not as detailed as compared with the Enhanced Monitoring feature in RDS. Take note as well that you do not have direct access to the instances/servers of your RDS database instance, unlike with your EC2 instances where you can install a CloudWatch agent or a custom script to get CPU and memory utilization of your instance.

The option that says: 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 is incorrect because the CPU% and MEM% metrics are not readily available in the Amazon RDS console, which is contrary to what is being stated in this option.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MonitoringOS.html#USER_Monitoring.OS.CloudWatchLogs

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch>

[Go back to Q377](#)

Answer to Q378: A

[Go back to Q378](#)

Explanation to Q378

CloudWatch has available Amazon EC2 Metrics for you to use for monitoring CPU utilization, Network utilization, Disk performance, and Disk Reads/Writes.

In case that you need to monitor the below items, you need to prepare a custom metric using a Perl or other shell script, as there are no ready to use metrics for these: Memory utilization, disk swap utilization, disk space utilization, page file utilization, log collection.

Take note that there is a multi-platform CloudWatch agent which can be installed on both Linux and Windows-based instances. You can use a single agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. This agent supports both Windows Server and Linux and enables you to select the metrics to be collected, including sub-resource metrics such as per-CPU core. It is recommended that you use the new agent instead of the older monitoring scripts to collect metrics and logs.

The option that says: Use the default CloudWatch configuration to your EC2 instances where the memory and disk utilization metrics are already available. Install the AWS Systems Manager (SSM) Agent to all your EC2 instances is incorrect because, by default, CloudWatch does not automatically provide memory and disk utilization metrics of your instances. You must set up custom CloudWatch metrics to monitor the memory, disk swap, disk space and page file utilization of your instances.

The option that says: Enable the Enhanced Monitoring option in EC2 and install CloudWatch agent to all of your EC2 instances to be able to view the memory and disk utilization in the CloudWatch dashboard is incorrect because Enhanced Monitoring is a feature of RDS and not of CloudWatch.

Using Amazon Inspector and installing the Inspector agent to all of your EC2 instances is incorrect because Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. It does not provide a custom metric to track the memory and disk utilization of each EC2 instance in your VPC.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

[Go back to Q378](#)

Answer to Q379: D

[Go back to Q379](#)

[Explanation to Q379](#)

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules. AWS KMS is integrated with most other AWS services that encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs.

The scenario mentions that you must encrypt the data before writing it to disk for storage. What this means is that you will have to temporarily store the data in memory and not persist it on the disk, then encrypt it on the fly before finally storing it. The result would be an encrypted data in your disk EBS Volume, and the EBS Encryption would be the secondary layer of protection/encryption for your sensitive data.

You can configure your application to use the KMS API to encrypt all data before saving it to disk. Hence, AWS KMS API is the correct answer.

Security Token Service is incorrect because AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-

privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). It is not used for encrypting data unlike KMS. EBS encryption is incorrect because although EBS encryption provides additional security for the EBS volumes, the application could not use this service to encrypt or decrypt each individual data that it writes on the disk. It is better to use KMS API instead to automatically encrypt the data before saving it to disk for maximum security, rather than after.

Elastic File System (EFS) is incorrect because EFS is a storage service and does not provide encryption services unlike KMS API.

References:

<https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>

[Go back to Q379](#)

Answer to Q380: A

[Go back to Q380](#)

Explanation to Q380

NA

[Go back to Q380](#)

Answer to Q381: D

[Go back to Q381](#)

Explanation to Q381

When you create a parameter group, the default WLM configuration contains one queue that can run up to five queries concurrently. You can add additional queues and configure WLM properties in each of them if you want more control over query processing. Each queue that you add has the same default WLM configuration until you configure its properties. When you add additional queues, the last queue in the configuration is the default queue. Unless a query is routed to another queue based on criteria in the WLM configuration, it is processed by the default queue. You cannot specify user groups or query groups for the default queue.

As with other parameters, you cannot modify the WLM configuration in the default parameter group. Clusters associated with the default parameter group always use the default WLM configuration. If you want to modify the WLM configuration, you must create a parameter group and then associate that parameter group with any clusters that require your custom WLM configuration.

Using the workload management (WLM) in the parameter group configuration is correct. In Amazon Redshift, you use workload management (WLM) to define the number of query queues that are available, and how queries are routed to those queues for processing. WLM is part of parameter group configuration. A cluster uses the WLM configuration that is specified in its associated parameter group.

The options that say: This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use RDS database instead and This is not possible with Redshift because it is not intended for OLAP application but rather, for OLTP. Use a NoSQL DynamoDB database instead are incorrect. Redshift is a good choice if you want to perform OLAP transactions in the cloud. On the contrary, RDS and DynamoDB are more suitable for OLTP applications.

Creating a Lambda function that can accept the number of query queues and using this value to control Redshift is incorrect since it will be too

costly and inefficient to use Lambda. Workload management (WLM) is a feature of Redshift that addresses the problem aptly.

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/workload-mgmt-config.html>

[Go back to Q381](#)

Answer to Q382: A, C

[Go back to Q382](#)

Explanation to Q382

NA

[Go back to Q382](#)

Answer to Q383: A

[Go back to Q383](#)

Explanation to Q383

NA

[Go back to Q383](#)

Answer to Q384: A

[Go back to Q384](#)

Explanation to Q384

Before we proceed in answering this question, we must first be clear with the actual definition of a "schema". Basically, the English definition of a schema is: a representation of a plan or theory in the form of an outline or model.

Just think of a schema as the "structure" or a "model" of your data in your database. Since the scenario requires that the schema, or the structure of your data, changes frequently, then you must pick a database which provides a non-rigid and flexible way of adding or removing new types of data. This is a classic example of choosing between a relational database and non-relational (NoSQL) database.

A relational database is known for having a rigid schema, with a lot of constraints and limits as to which (and what type of) data can be inserted or not. It is primarily used for scenarios where you must support complex queries which fetch data across several tables. It is best for scenarios where you have complex table relationships but for use cases where you need to have a flexible schema, this is not a suitable database to use.

For NoSQL, it is not as rigid as a relational database because you can easily add or remove rows or elements in your table/collection entry. It also has a more flexible schema because it can store complex hierarchical data within a single item which, unlike a relational database, does not entail changing multiple related tables. Hence, the best answer to be used here is a NoSQL database, like DynamoDB. When your business requires a low-latency response to high-traffic queries, taking advantage of a NoSQL system generally makes technical and economic sense.

Amazon DynamoDB helps solve the problems that limit the relational system scalability by avoiding them. In DynamoDB, you design your schema specifically to make the most common and important queries as fast and as inexpensive as possible. Your data structures are tailored to the specific requirements of your business use cases.

Remember that a relational database system does not scale well for the following reasons:

- It normalizes data and stores it on multiple tables that require multiple queries to write to disk.
- It generally incurs the performance costs of an ACID-compliant transaction system.
- It uses expensive joins to reassemble required views of query results.

For DynamoDB, it scales well due to these reasons:- Its schema flexibility lets DynamoDB store complex hierarchical data within a single item.

DynamoDB is not a totally schema-less database since the very definition of a schema is just the model or structure of your data.- Composite key design lets it store related items close together on the same table.

An Amazon RDS instance in Multi-AZ Deployments configuration and an Amazon Aurora database with Read Replicas are incorrect because both are a type of relational database.

Redshift is incorrect because it is primarily used for OLAP systems.

References:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-general-nosql-design.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-relational-modeling.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQltoNoSQL.html>

[Go back to Q384](#)

Answer to Q385: A, E

[Go back to Q385](#)

Explanation to Q385

Amazon EC2 provides you access to the operating system of the instance that you created.

Amazon EMR provides you a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances. You can access the operating system of these EC2 instances that were created by Amazon EMR.

Amazon Athena, DynamoDB, and Amazon Neptune are incorrect as these are managed services, which means that AWS manages the underlying operating system and other server configurations that these databases use.

References:

<https://aws.amazon.com/ec2/> <https://aws.amazon.com/emr/>

[Go back to Q385](#)

Answer to Q386: D

[Go back to Q386](#)

Explanation to Q386

NA

[Go back to Q386](#)

Answer to Q387: B

[Go back to Q387](#)

Explanation to Q387

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.

Amazon ElastiCache is incorrect because although you may use ElastiCache as your database cache, it will not reduce the DynamoDB response time from milliseconds to microseconds as compared with DynamoDB DAX. AWS Device Farm is incorrect because this is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.

DynamoDB Auto Scaling is incorrect because this is primarily used to automate capacity management for your tables and global secondary indexes.

References:

<https://aws.amazon.com/dynamodb/dax>

<https://aws.amazon.com/device-farm>

[Go back to Q387](#)

Answer to Q388: C

[Go back to Q388](#)

Explanation to Q388

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different

Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

In this scenario, the best RDS configuration to use is an Oracle database in RDS with Multi-AZ deployments to ensure high availability even if the primary database instance goes down. Hence, creating an Oracle database in RDS with Multi-AZ deployments is the correct answer.

Launching an Oracle database instance in RDS with Recovery Manager (RMAN) enabled and launching an Oracle Real Application Clusters (RAC) in RDS are incorrect because Oracle RMAN and RAC are not supported in RDS.

Migrating your Oracle data to Amazon Aurora by converting the database schema using AWS Schema Conversion Tool and AWS Database Migration Service is incorrect because although this solution is feasible, it takes time to migrate your Oracle database to Aurora which is not acceptable. Based on this option, the Aurora database does not have a Read Replica and is not configured as an Amazon Aurora DB cluster, which could have improved the availability of the database.

References:

<https://aws.amazon.com/rds/details/multi-az/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

[Go back to Q388](#)

Answer to Q389: D

[Go back to Q389](#)

Explanation to Q389

Since the company is using Microsoft Active Directory which implements Security Assertion Markup Language (SAML), you can set up a SAML-Based Federation for API Access to your AWS cloud. In this way, you can easily connect to AWS using the login credentials of your on-premises network.

AWS supports identity federation with SAML 2.0, an open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. By using SAML, you can simplify the process of configuring federation with AWS, because you can use the IdP's service instead of writing custom identity proxy code.

Before you can use SAML 2.0-based federation as described in the preceding scenario and diagram, you must configure your organization's IdP and your AWS account to trust each other. The general process for configuring this trust is described in the following steps. Inside your organization, you must have an IdP that supports SAML 2.0, like Microsoft Active Directory Federation Service (AD FS, part of Windows Server), Shibboleth, or another compatible SAML 2.0 provider.

Hence, the correct answer is: Set up SAML 2.0-Based Federation by using a Microsoft Active Directory Federation Service (AD FS). Setting up SAML 2.0-Based Federation by using a Web Identity Federation is incorrect because this is primarily used to let users sign in via a well-known external identity provider (IdP), such as Login with Amazon, Facebook, Google. It does not utilize Active Directory.

Using IAM users is incorrect because the situation requires you to use the existing credentials stored in their Active Directory, and not user accounts

that will be generated by IAM.

Using Amazon VPC is incorrect because this only lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This has nothing to do with user authentication or Active Directory.

References:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

[Go back to Q389](#)

Answer to Q390: B

[Go back to Q390](#)

Explanation to Q390

EBS snapshots occur asynchronously which makes the option that says: The volume can be used as normal while the snapshot is in progress the correct answer.

This means that the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume hence, you can still use the volume.

The rest of the options are incorrect because you will still be able to perform normal read and write operations on your EBS volume even while a snapshot is ongoing. Although you can take a snapshot of a volume while a previous snapshot of that volume is in the pending status, having multiple pending snapshots of a volume may result in reduced volume performance until the snapshots complete.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

[Go back to Q390](#)

Answer to Q391: A

[Go back to Q391](#)

Explanation to Q391

In this question, you should take note of the two keywords/phrases: "file operation" and "allows concurrent connections from multiple EC2 instances". There are various AWS storage options that you can choose but whenever these criteria show up, always consider using EFS instead of using EBS Volumes which is mainly used as a "block" storage and can only have one connection to one EC2 instance at a time. Amazon EFS provides the scale and performance required for big data applications that require high throughput to compute nodes coupled with read-after-write consistency and low-latency file operations. Amazon EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and supports full file system access semantics (such as strong consistency and file locking).

Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available.

Option B is incorrect because EBS does not allow concurrent connections from multiple EC2 instances hosted on multiple AZs and it does not store data redundantly across multiple AZs by default, unlike EFS.

Option C is incorrect because although S3 can handle concurrent connections from multiple EC2 instances, it does not have the ability to provide low-latency file operations, which is required in this scenario.

Option D is incorrect because Glacier is an archiving storage solution and is not applicable in this scenario.

References:

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

<https://aws.amazon.com/efs/faq/>

[Go back to Q391](#)

Answer to Q392: C

[Go back to Q392](#)

Explanation to Q392

You can use path conditions to define rules that forward requests to different target groups based on the URL in the request (also known

as path-based routing). This type of routing is the most appropriate solution for this scenario hence, Option C is correct.

Each path condition has one path pattern. If the URL in a request matches the path pattern in a listener rule exactly, the request is routed using that rule. A path pattern is case-sensitive, can be up to 128 characters in length, and can contain any of the following characters. You can include up to three wildcard characters. AZ, az, 09 _ - . \$ / ~ " ' @ : + & (using &) * (matches 0 or more characters) ? (matches exactly 1 character) Example path patterns /img/* /js/*

Option A is incorrect because host-based routing defines rules that forward requests to different target groups based on the host name in the host header instead of the URL, which is what is needed in this scenario.

Option B is incorrect because a Classic Load Balancer does not support path-based routing. You must use an Application Load Balancer.

Option D is incorrect because a Network Load Balancer is used for applications that need extreme network performance and static IP.

It also does not support path-based routing which is what is needed in this scenario. Furthermore, the statement mentions host-based routing yet, the description is about path-based routing.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html#application-load-balancer-benefits>

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#path-conditions>

[Go back to Q392](#)

Answer to Q393: C

[Go back to Q393](#)

Explanation to Q393

NA

[Go back to Q393](#)

Answer to Q394: D

[Go back to Q394](#)

Explanation to Q394

Option D is correct. Horizontal scaling means increasing the number of your message producers (making SendMessage requests) and consumers (making ReceiveMessage and DeleteMessage requests) in order to increase your overall queue throughput. You can scale horizontally by increasing the number of threads on a client, adding clients, or both. You should achieve essentially linear gains in queue throughput as you add more clients. For example, if you double the number of clients, you can get twice the throughput.

Reference:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-throughput-horizontal-scaling-and-batching.html>

[Go back to Q394](#)

Answer to Q395: A, C

[Go back to Q395](#)

Explanation to Q395

NA

[Go back to Q395](#)

Answer to Q396: D

[Go back to Q396](#)

Explanation to Q396

NA

[Go back to Q396](#)

Answer to Q397: C

[Go back to Q397](#)

Explanation to Q397

NA

[Go back to Q397](#)

Answer to Q398: A

[Go back to Q398](#)

Explanation to Q398

By default, each workflow execution can run for a maximum of 1 year in Amazon SWF. This means that it is possible that in your workflow, there are some tasks which require manual action that renders it idle. As a result, some orders get stuck for almost 4 weeks. Amazon SWF does not take any special action if a workflow execution is idle for an extended period. Idle executions are subject to the timeouts that you configure. For example, if you have set the maximum duration for an execution to be 1 day, then an idle execution will be timed out if it exceeds the 1-day limit. Idle executions

are also subject to the Amazon SWF limit on how long an execution can run (1 year).

Options B and C are incorrect as the maximum execution time is 1 year.

Option D is incorrect as there is no problem with SWF, and you can't manually restart this service.

Reference:

<https://aws.amazon.com/swf/>

[Go back to Q398](#)

Answer to Q399: B

[Go back to Q399](#)

Explanation to Q399

One thing that you must notice here is that the company is using Multi-AZ databases in all their environments, including their development and test environment. This is costly and unnecessary as these two environments are not critical. It is better to use Multi-AZ for production environments to reduce costs.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q399](#)

Answer to Q400: A

[Go back to Q400](#)

Explanation to Q400

NA

[Go back to Q400](#)

Answer to Q401: A

[Go back to Q401](#)

Explanation to Q401

Amazon Aurora MySQL and Amazon Aurora PostgreSQL support Amazon Aurora Replicas, which share the same underlying volume as the primary instance. Updates made by the primary are visible to all Amazon Aurora Replicas. With Amazon Aurora MySQL, you can also create MySQL Read Replicas based on MySQL's binlog-based replication engine. In MySQL Read Replicas, data from your primary instance is replayed on your replica as transactions. For most use cases, including read scaling and high availability, we recommend using Amazon Aurora Replicas. Hence, the right answer here is Option A.

Option B is incorrect because Aurora is a database engine for RDS and not deployed on a typical EC2 instance.

Option C is incorrect because Hash Joins are mainly used if you need to join a large amount of data by using an equijoin and not for improving availability.

Option D is incorrect because the Asynchronous Key Prefetch is mainly used to improve the performance of queries that join tables across indexes.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL_BestPractices.html

<https://aws.amazon.com/rds/aurora/faqs/>

[Go back to Q401](#)

Answer to Q402: B

[Go back to Q402](#)

Explanation to Q402

Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume
- All volumes created from those snapshots

In this scenario, the EBS volume attached to the instance is already unencrypted. The best way to encrypt the data is to create and mount a new, encrypted Amazon EBS volume. Then move the data to the new volume and finally, delete the old, unencrypted Amazon EBS volume. Hence, Option B is the correct answer.

Option A is incorrect because a step is missing for this option to be a valid answer. You need to copy the snapshot first while applying encryption parameters, for the resulting target snapshot to be encrypted before restoring it to a new encrypted EBS volume.

Option C is incorrect because you cannot encrypt the volume even if you unmount the volume. Remember that encryption must be done during volume creation.

Option D is incorrect because you cannot create an encrypted snapshot of an unencrypted volume or change existing volume from unencrypted to encrypted. You must create new encrypted volume and transfer data to the new volume.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

[Go back to Q402](#)

Answer to Q403: B

[Go back to Q403](#)

Explanation to Q403

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency. To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or apex.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Route 53 responds with the value from the selected record, such as the IP address for a web server.

References:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/TutorialAdingLBRRegion.html>

[Go back to Q403](#)

Answer to Q404: A

[Go back to Q404](#)

Explanation to Q404

To use the AWS Management Console, IAM users must provide their account ID or account alias in addition to their username and password. When you, as an administrator, create an IAM user in the console, you must send the sign-in credentials to that user, including the username and the URL to the account sign-in page. Your unique account sign-in page URL is created automatically when you begin using IAM. You do not have to do anything to use this sign-in page. You can also customize the account sign-in URL for your account if you want the URL to contain your company name (or other friendly identifier) instead of your AWS account ID number.

AWS sign-in page URL format:

https://My_AWS_Account_ID.signin.aws.amazon.com/console/

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/console.html>

[Go back to Q404](#)

Answer to Q405: A, D

[Go back to Q405](#)

Explanation to Q405

Server-side encryption is about data encryption at rest, i.e., Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. If you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

For example, if you share your objects using a pre-signed URL, that URL works the same way for both encrypted and unencrypted objects. You have three mutually exclusive options depending on how you choose to manage the encryption keys: Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) Use Server-Side Encryption with Customer-Provided Keys (SSE-C) Options A and D are correct because they are using Amazon S3-Managed Keys (SSE-S3) and Customer-Provided Keys (SSE-C). SSE-S3 uses AES-256 encryption and SSE-C allows you to use your own encryption key.

Options B and C are incorrect because both options use EBS encryption and not S3.

Option E is incorrect as S3 doesn't provide AES-128 encryption, only AES-256.

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

[Go back to Q405](#)

Answer to Q406: A

[Go back to Q406](#)

Explanation to Q406

By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance. To implement the sticky session feature, you need to have

2 things: An HTTP/HTTPS load balancer. At least one healthy instance in each Availability Zone. The key to managing sticky sessions is to determine how long your load balancer should consistently route the user's request to the same instance. If your application has its own session cookie, then you can configure Elastic Load Balancing so that the session cookie follows the duration specified. If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration. With the sticky session feature, it is possible to instruct the load balancer to route repeated requests to the same EC2 instance whenever possible.

Take note that these 2 types of EC2 instances are NOT required when you want to implement the sticky session. They are mainly used to improve the performance of your EC2 instances but not necessarily helpful for the feature. EC2 instance with Enhanced Networking An EC2 instance with a RAID volume

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>

[Go back to Q406](#)

Answer to Q407: C, D

[Go back to Q407](#)

Explanation to Q407

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

Amazon S3 supports the following destinations where it can publish events:

1. Amazon Simple Notification Service (Amazon SNS) topic - A web service that coordinates and manages the delivery or sending of messages to the subscribing endpoints or clients.
2. Amazon Simple Queue Service (Amazon SQS) queue - Offers reliable and scalable hosted queues for storing messages as they travel between computer.
3. AWS Lambda - AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure.

You package up and upload your custom code to AWS Lambda when you create a Lambda function Option A is incorrect because Amazon Kinesis is used to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information, and not used for event notifications. You must use SNS, SQS or Lambda.

Option B is incorrect because SES is mainly used for sending emails designed to help digital marketers and application developers send marketing, notification, and transactional emails, and not for sending event notifications from S3. You must use SNS, SQS or Lambda.

Option E is incorrect because SWF is mainly used to build applications that use Amazon's cloud to coordinate work across distributed components and not used to trigger event notifications from S3.

You must use SNS, SQS or Lambda. Here's what you need to do in order to start using this new feature with your application: Create the queue, topic, or Lambda function (which I'll call the target for brevity) if necessary. Grant S3 permission to publish to the target or invoke the Lambda function. For SNS or SQS, you do this by applying an appropriate policy to the topic or the queue. For Lambda, you must create and supply an IAM role, then associate it with the Lambda function. Arrange for your application to be

invoked in response to activity on the target. As you will see in a moment, you have several options here. Set the buckets Notification Configuration to point to the target.

Reference :

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

[Go back to Q407](#)

Answer to Q408: B, C

[Go back to Q408](#)

Explanation to Q408

You can secure the privacy of your data in AWS, both at rest and in-transit, through encryption. If your data is stored in EBS Volumes, you can enable EBS Encryption and if it is stored on Amazon S3, you can enable client-side and server-side encryption.

Option D is incorrect as public data sets are designed to be publicly accessible.

Options A and E are incorrect as there is no such thing as On-Premise Data Encryption for S3 and EBS as these services are in the AWS cloud and not on your on-premise network.

References:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html>

[Go back to Q408](#)

Answer to Q409: A

[Go back to Q409](#)

Explanation to Q409

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and responds instantly instead of having to wait until all your data is collected before the processing can begin.

Option B is incorrect because Redshift Spectrum is primarily used to directly query open data formats stored in Amazon S3 without the need for unnecessary data movement, which enables you to analyze data across your data warehouse and data lake, together, with a single service. It does not provide the ability to process your data in real-time, unlike Kinesis. Option C is incorrect because AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It does not provide the ability to process your data in real-time, unlike Kinesis.

Option D is incorrect because Amazon EMR is a web service that uses an open-source Hadoop framework, to quickly & cost-effectively process vast

amounts of data. It does not provide the ability to process your data in real-time, unlike Kinesis.

Reference:

<https://aws.amazon.com/kinesis/>

[Go back to Q409](#)

Answer to Q410: A

[Go back to Q410](#)

Explanation to Q410

NA

[Go back to Q410](#)

Answer to Q411: A

[Go back to Q411](#)

Explanation to Q411

CloudWatch has available Amazon EC2 Metrics for you to use for monitoring CPU utilization, Network utilization, Disk performance and Disk Reads/Writes.

In case that you need to monitor the below items, you need to prepare a custom metric using a Perl or other shell script, as there are no ready to use metrics for these: memory utilization, disk swap utilization, disk space utilization, page file utilization, log collection.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

[Go back to Q411](#)

Answer to Q412: C

[Go back to Q412](#)

Explanation to Q412

NA

[Go back to Q412](#)

Answer to Q413: B, D

[Go back to Q413](#)

Explanation to Q413

DynamoDB supports key-value and document data structures. A key-value store is a database service that provides support for storing, querying, and updating collections of objects that are identified using a key and values that contain the actual content being stored. Meanwhile, a document data store provides support for storing, querying, and updating items in a document format such as JSON, XML, and HTML. The DynamoDB Time-to-Live (TTL) mechanism enables you to manage web sessions of your application easily. It lets you set a specific timestamp to delete expired items from your tables. Once the timestamp expires, the corresponding item is marked as expired and is subsequently deleted from the table. By using this functionality, you do not have to track expired data and delete it.

manually. TTL can help you reduce storage usage and reduce the cost of storing data that is no longer relevant. Amazon DynamoDB stores structured data indexed by primary key and allow low latency read and write access to items ranging from 1 byte up to 400KB. Amazon S3 stores unstructured blobs and is suited for storing large objects up to 5 TB. In order to optimize your costs across AWS services, large objects or infrequently accessed data sets should be stored in Amazon S3, while smaller data elements or file pointers (possibly to Amazon S3 objects) are best saved in Amazon DynamoDB. To speed up access to relevant data, you can pair Amazon S3 with a search engine such as Amazon CloudSearch or a database such as Amazon DynamoDB or Amazon RDS. In these scenarios, Amazon S3 stores the actual information, and the search engine or database serves as the repository for associated metadata such as the object name, size, keywords, and so on. Metadata in the database can easily be indexed and queried, making it very efficient to locate an objects reference by using a search engine or a database query. This result can be used to pinpoint and retrieve the object itself from Amazon S3.

References :

<https://aws.amazon.com/dynamodb/faqs/>

<https://d1.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=9>

[Go back to Q413](#)

Answer to Q414: B

[Go back to Q414](#)

Explanation to Q414

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security

features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the AWS Cloud for scalable and cost-effective storage that helps maintain data security.

Reference :

<http://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

[Go back to Q414](#)

Answer to Q415: D

[Go back to Q415](#)

Explanation to Q415

Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

Option A is incorrect. DynamoDB is a NoSQL database which is based on key-value pairs used for fast processing of small data that dynamically grows and changes. But if you need to scan large amounts of data (i.e. a lot of keys all in one query), the performance will not be optimal.

Option B is incorrect because ElastiCache is used to increase the performance, speed and redundancy with which applications can retrieve data by providing an in-memory database caching system, and not for database analytical processes.

Option C is incorrect because RDS is mainly used for On-Line Transaction Processing (OLTP) applications and not for Online Analytics Processing

(OLAP).

References:

<https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html>

<https://docs.aws.amazon.com/redshift/latest/gsg/getting-started.html>

[Go back to Q415](#)

Answer to Q416: C

[Go back to Q416](#)

Explanation to Q416

Remember that the AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in these five categories: Cost Optimization, Performance, Fault Tolerance, Security, and Service Limits. You can use a mnemonic, such as CPFSS, to memorize these five categories.

Reference:

<https://aws.amazon.com/premiumsupport/trustedadvisor/>

[Go back to Q416](#)

Answer to Q417: B

[Go back to Q417](#)

Explanation to Q417

NA

[Go back to Q417](#)

Answer to Q418: C

[Go back to Q418](#)

Explanation to Q418

An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet and prevents the Internet from initiating an IPv6 connection with your instances. Take note that an egress-only Internet gateway is for use with IPv6 traffic only. To enable outbound-only Internet communication over IPv4, use a NAT gateway instead.

Reference:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

[Go back to Q418](#)

Answer to Q419: D

[Go back to Q419](#)

Explanation to Q419

NA

[Go back to Q419](#)

Answer to Q420: C

[Go back to Q420](#)

Explanation to Q420

NA

[Go back to Q420](#)

Answer to Q421: A

[Go back to Q421](#)

Explanation to Q421

When the word durability pops out, the first service that should come to your mind is Amazon S3. Since this service is not available in the answer options, we can look at the other data store available which is Amazon DynamoDB. DynamoDB is durable, scalable, and highly available data store which can be used for real-time tabulation. You can also use AppSync with DynamoDB to make it easy for you to build collaborative apps that keep shared data updated in real time. You just specify the data for your app with simple code statements and AWS AppSync manages everything needed to keep the app data updated in real time. This will allow your app to access data in Amazon DynamoDB, trigger AWS Lambda functions, or run Amazon Elasticsearch queries and combine data from these services to provide the exact data you need for your app.

Option B is incorrect as Amazon Redshift is mainly used as a data warehouse and for online analytic processing (OLAP). Although this service can be used for this scenario, DynamoDB is still the top choice given its better durability and scalability.

Options C and D are possible answers in this scenario, however, DynamoDB is much more suitable for simple mobile apps which do not have complicated data relationships compared with enterprise web applications. The scenario says that the mobile app will be used from around the world,

which is why you need a data storage service which can be supported globally. It would be a management overhead to implement multi-region deployment for your RDS and Aurora database instances compared to using the Global table feature of DynamoDB.

References:

<https://aws.amazon.com/dynamodb/faqs/>

<https://aws.amazon.com/appsync/>

[Go back to Q421](#)

Answer to Q422: A

[Go back to Q422](#)

Explanation to Q422

An elastic network interface (ENI) is a logical networking component in a VPC that represents a virtual network card. You can attach a network interface to an EC2 instance in the following ways: When it's running (hot attach) When it's stopped (warm attach) When the instance is being launched (cold attach).

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#attach_eni_launch

[Go back to Q422](#)

Answer to Q423: A, B

[Go back to Q423](#)

Explanation to Q423

If you got your certificate from a third-party CA, import the certificate into ACM or upload it to the IAM certificate store. Hence, Options 1 and 2 are the correct answers. ACM lets you import third-party certificates from the ACM console, as well as programmatically. If ACM is not available in your region, use AWS CLI to upload your third-party certificate to the IAM certificate store.

Options C and D are incorrect as S3 is not a suitable service to store the SSL certificate. Option E is incorrect because although you can upload certificates to CloudFront, it doesn't mean that you can import SSL certificates on it. You would not be able to export the certificate that you have loaded in CloudFront nor assign them to your EC2 or ELB instances as it would be tied to a single CloudFront distribution.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html#cnames-and-https-uploading-certificates>

[Go back to Q423](#)

Answer to Q424: B, D

[Go back to Q424](#)

Explanation to Q424

Amazon EC2 Auto Scaling provides you with an option to enable automatic scaling for one or more EC2 instances by attaching them to your existing

Auto Scaling group. After the instances are attached, they become a part of the Auto Scaling group.

The instance that you want to attach must meet the following criteria:

- The instance is in the running state
- The AMI used to launch the instance must still exist
- The instance is not a member of another Auto Scaling group
- The instance is launched into one of the Availability Zones defined in your Auto Scaling group
- If the Auto Scaling group has an attached load balancer, the instance and the load balancer must both be in EC2-Classic or the same VPC.

If the Auto Scaling group has an attached target group, the instance and the load balancer must both be in the same VPC.

Based on the above criteria, Options 2 and 4 are the correct answers.

Reference:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/attach-instance-asg.html>

[Go back to Q424](#)

Answer to Q425: B

[Go back to Q425](#)

Explanation to Q425

NA

[Go back to Q425](#)

Answer to Q426: A

[Go back to Q426](#)

Explanation to Q426

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, API calls, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Option B is incorrect because although CloudWatch is also a monitoring service, it cannot track the API calls to your AWS resources.

Option C is incorrect because AWS X-Ray is not a suitable service to use to track each API call to your AWS resources. It just helps you debug and analyze your microservices applications with request tracing so you can find the root cause of issues and performance.

Option D is incorrect because Redshift Spectrum is not a monitoring service but rather a feature of Amazon Redshift that enables you to query and analyze all of your data in Amazon S3 using the open data formats you already use, with no data loading or transformations needed.

Reference:

<https://aws.amazon.com/cloudtrail/>

[Go back to Q426](#)

Answer to Q427: A, B

[Go back to Q427](#)

Explanation to Q427

In this scenario, the correct answers are:

- Enable Multi-Factor Authentication
- Assign an IAM role to the Amazon EC2 instance Always remember that you should associate IAM roles to EC2 instances and not an IAM user, for the purpose of accessing other AWS services.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your username and password. With MFA enabled, when a user signs into an AWS website, they will be prompted for their user name and password (the first factor, what they know), as well as for an authentication code from their AWS MFA device (the second factor, what they have).

Taken together, these multiple factors provide increased security for your AWS account settings and resources. You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can also be used to control access to AWS service APIs.

References:

<https://aws.amazon.com/iam/details/mfa/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

[Go back to Q427](#)

Answer to Q428: D

[Go back to Q428](#)

Explanation to Q428

To achieve this requirement, you can deploy your Oracle database to Amazon EC2 instances with data replication between two different Availability Zones. Hence, option D is the correct answer.

The deployment of this architecture can easily be achieved by using CloudFormation and Quick Start. Please refer to the reference link for information. The Quick Start deploys the Oracle primary database (using the preconfigured, general-purpose starter database from Oracle) on an Amazon EC2 instance in the first Availability Zone. It then sets up a second EC2 instance in a second Availability Zone, copies the primary database to the second instance by using the DUPLICATE command, and configures Oracle Data Guard.

Options A and B are incorrect because the scenario requires you to have access to the underlying operating system of the database server. Remember that Amazon RDS is a managed database service, which means that Amazon is the one that manages the underlying operating system of the database instance and not you.

Option C is incorrect since deploying to just one Availability Zone (AZ) will not make the database tier highly available. If that AZ went down, your database will be unavailable.

References :

<https://aws.amazon.com/quickstart/>

<https://docs.aws.amazon.com/quickstart/latest/oracle-database/architecture.html>

http://docs.aws.amazon.com/dms/latest/userguide/CHAP_Introduction.ReplicationInstance.html

[Go back to Q428](#)

Answer to Q429: B

[Go back to Q429](#)

[Explanation to Q429](#)

NA

[Go back to Q429](#)

Answer to Q430: A

[Go back to Q430](#)

[Explanation to Q430](#)

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

Reference:

<https://aws.amazon.com/opsworks/>

[Go back to Q430](#)

Answer to Q431: A

[Go back to Q431](#)

Explanation to Q431

NA

[Go back to Q431](#)

Answer to Q432: A

[Go back to Q432](#)

Explanation to Q432

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival which is cheaper than Amazon S3. The standard retrievals in Glacier allow you to access any of your archives within several hours. Standard retrievals typically complete within 3–5 hours, which is well within the required 24-hour data retrieval time in the scenario.

Reference:

<https://aws.amazon.com/glacier/faqs/>

[Go back to Q432](#)

Answer to Q433: A, C

[Go back to Q433](#)

Explanation to Q433

Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance terminates, which could occur through a web services command, by running "shutdown -h", or through instance failure. When you stop an instance, AWS shuts it down but don't charge hourly usage for a stopped instance or data transfer fees, but AWS does charge for the storage of any Amazon EBS volumes.

Hence, options A and C are the right answers and conversely, options B and F are incorrect as there is no charge for a terminated EC2 instance that you have shut down.

Option D is incorrect because there are no additional charges for creating and using the VPC itself. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges.

Option E is incorrect since Amazon stores the data sets at no charge to the community and, as with all AWS services, you pay only for the compute and storage you use for your own applications.

References:

<https://aws.amazon.com/cloudtrail/>

<https://aws.amazon.com/vpc/faqs>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-public-data-sets.html>

[Go back to Q433](#)

Answer to Q434: C

[Go back to Q434](#)

[Explanation to Q434](#)

Amazon EC2 uses public key cryptography to encrypt and decrypt login information. Public key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data.

The public and private keys are known as a key pair. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. On a Linux instance, the public key content is placed in an entry within `~/.ssh/authorized_keys`. This is done at boot time and enables you to securely access your instance using the private key instead of a password.

Options A and B are incorrect as both Custom EC2 password and EC2 Connection Strings do not exist.

Option D is incorrect as Access Keys are used for API calls and not for logging in to EC2.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

[Go back to Q434](#)

Answer to Q435: A, C

[Go back to Q435](#)

Explanation to Q435

The global news website has a problem with latency considering that there are a lot of readers of the site from all parts of the globe. In this scenario, you can use a content delivery network (CDN) which is a geographically

distributed group of servers which work together to provide fast delivery of Internet content. And since this is a news website, most of its data are read-only, which can be cached to improve the read throughput and avoid the repetitive requests from the server. In AWS, Amazon CloudFront is the global content delivery network (CDN) service that you can use and for web caching, Amazon ElastiCache is the suitable service.

Hence, the answers here are options A and C.

Option B is incorrect as AWS Storage Gateway is used for storage.

Option D is incorrect as this would be costly and totally unnecessary considering that you can use Amazon CloudFront and ElastiCache to improve the performance of the website.

References:

<https://aws.amazon.com/elasticsearch/>

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

[Go back to Q435](#)

Answer to Q436: A, C

[Go back to Q436](#)

Explanation to Q436

If you use PuTTY to connect to your instance via SSH and get either of the following errors, Error: Server refused our key or Error: No supported authentication methods available, verify that you are connecting with the appropriate user name for your AMI. Enter the username in the Username box in the PuTTY Configuration window. The appropriate usernames are as follows:

- For an Amazon Linux AMI, the username is ec2-user.

- For a RHEL AMI, the username is ec2-user or root.
- For an Ubuntu AMI, the username is ubuntu or root.
- For a Centos AMI, the username is centos.
- For a Debian AMI, the username is admin or root.
- For a Fedora AMI, the user name is ec2-user.
- For a SUSE AMI, the user name is ec2-user or root.

Otherwise, if ec2-user and root don't work, check with the AMI provider. You should also verify that your private key (.pem) file has been correctly converted to the format recognized by PuTTY (.ppk).

Options B and D are incorrect because both an IAM user and IAM role policy have nothing to do with this issue.

Option E is incorrect because you don't need to wait an hour in order to connect to a new EC2 instance as you can immediately connect to it once it is created.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#TroubleshootingInstancesConnectingPuTTY>

[Go back to Q436](#)

Answer to Q437: A

[Go back to Q437](#)

Explanation to Q437

Amazon API Gateway provides throttling at multiple levels including global and by a service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs and configure Amazon API

Gateway to handle a burst of 2,000 requests per second for a few seconds. Amazon API Gateway tracks the number of requests per second. Any requests over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response.

Option B is incorrect because although it can scale using AWS Edge locations, you still need to configure the throttling to further manage the bursts of your APIs.

Option C is incorrect because API Gateway is a fully managed service and hence, you do not have access to its underlying resources.

Option D is incorrect because RDS has Multi-AZ and Read Replica capabilities, and not API Gateway.

Reference:

https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching

[Go back to Q437](#)

Answer to Q438: D

[Go back to Q438](#)

Explanation to Q438

`http://169.254.169.254/latest/meta-data/` is the URL that you can use to retrieve the Instance Metadata of your EC2 instance, including the public-hostname, public-ipv4, public-keys, et cetera. This can be helpful when you're writing scripts to run from your instance as it enables you to access the local IP address of your instance from the instance metadata to manage a connection to an external application. Remember that you are

not billed for HTTP requests used to retrieve instance metadata and user data.

Options A and Option B are incorrect because the URLs are incorrect - the numbers are not in the correct order.

Option C is incorrect because it refers to the loopback Internet protocol (IP) address.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

[Go back to Q438](#)

Answer to Q439: D

[Go back to Q439](#)

Explanation to Q439

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. The master keys that you create in AWS KMS are protected by FIPS 140-2 validated cryptographic modules. AWS KMS is integrated with most other AWS services that encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide encryption key usage logs to help meet your auditing, regulatory and compliance needs. In this scenario, you can configure your application to use the KMS API to encrypt all data before saving it to disk.

Hence, Option D is the correct answer.

Option A is incorrect because AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). It is not used for encrypting data unlike KMS.

Option B is incorrect because although EBS encryption provides additional security for the EBS volumes, the application could not use this service to encrypt or decrypt each individual data that it writes on the disk. It is better to use KMS API instead to automatically encrypt the data before saving it to disk.

Option C is incorrect because EFS is a storage service and does not provide encryption services unlike KMS API.

Reference:

<https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html>

[Go back to Q439](#)

Answer to Q440: C

[Go back to Q440](#)

Explanation to Q440

To meet the requirement on this scenario, you can just maintain a single snapshot of the EBS volume since its latest snapshot is both incremental and complete. You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage

costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all the information needed to restore your data (from the moment the snapshot was taken) to a new EBS volume.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

[Go back to Q440](#)

Answer to Q441: A, B

[Go back to Q441](#)

Explanation to Q441

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Unlike other Amazon object storage classes, which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ. Because of this, storing data in S3 One Zone-IA costs 20% less than storing it in S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower cost option for infrequently accessed data but do not require the availability and resilience of S3 Standard or S3 Standard-IA storage. It's a good choice, for example, for storing secondary backup copies of on-premises data or easily re-creatable data, or for storage used as an S3 Cross-Region Replication target from another AWS Region. S3 One Zone-IA offers the same high durability, high throughput, and low latency of Amazon S3 Standard and S3 Standard-IA, with a low per GB storage price and per GB retrieval fee. The S3 One Zone-IA storage class is set at the object level and can exist in the same bucket as S3 Standard and S3 Standard-IA, allowing you to use S3 Lifecycle Policies to automatically

transition objects between storage classes without any application changes. Key Features:

- Same low latency and high throughput performance of S3 Standard and S3 Standard-IA
- Designed for durability of 99.99999999% of objects in a single Availability Zone, but data will be lost in the event of Availability Zone destruction
- Designed for 99.5% availability over a given year -Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL for data in transit and encryption of data at rest -Lifecycle management for automatic migration of objects

Remember that since the S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.

Reference:

https://aws.amazon.com/s3/storage-classes/#Amazon_S3_One_Zone_Infrequent_Access

[Go back to Q441](#)

Answer to Q442: B, D

[Go back to Q442](#)

Explanation to Q442

You can store session state data on both DynamoDB and ElastiCache. These AWS services provide high performance storage of key-value pairs which can be used to build a highly available web application.

References:

<https://aws.amazon.com/caching/database-caching/>

<https://aws.amazon.com/caching/session-management/>

[Go back to Q442](#)

Answer to Q443: B

[Go back to Q443](#)

Explanation to Q443

Although an AWS Snowball device costs less than AWS Snowball Edge, it cannot store 80 TB of data in one device. Take note that the storage capacity is different from the usable capacity for Snowball and Snowball Edge. Remember that an 80 TB Snowball appliance and 100 TB Snowball Edge appliance only have 72 TB and 83 TB of usable capacity respectively. Hence, it would be costly if you use two Snowball devices compared to using just one AWS Snowball Edge device. The AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud. Each Snowball Edge device can transport data at speeds faster than the internet. This transport is done by shipping the data in the appliances through a regional carrier. The appliances are rugged shipping containers, complete with E Ink shipping labels. The AWS Snowball Edge device differs from the standard Snowball because it can bring the power of the AWS Cloud to your on-premises location, with local storage and compute functionality. Snowball Edge devices have three options for device configurations storage optimized, compute optimized, and with GPU. When this guide refers to Snowball Edge devices, it's referring to all options of the device. Whenever specific information

applies only to one or more optional configurations of devices, like how the Snowball Edge with GPU has an on-board GPU, it will be called out.

References:

<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>

<https://docs.aws.amazon.com/snowball/latest/ug/device-differences.html>

[Go back to Q443](#)

Answer to Q444: A

[Go back to Q444](#)

Explanation to Q444

To control the versions of files that are served from your distribution, you can either invalidate files or give them versioned file names. If you want to update your files frequently, AWS recommends that you primarily use file versioning for the following reasons:

- Versioning enables you to control which file a request returns even when the user has a version cached either locally or behind a corporate caching proxy. If you invalidate the file, the user might continue to see the old version until it expires from those caches.
- CloudFront access logs include the names of your files, so versioning makes it easier to analyze the results of file changes.
- Versioning provides a way to serve different versions of files to different users.
- Versioning simplifies rolling forward and back between file revisions.
- Versioning is less expensive. You still must pay for CloudFront to transfer new versions of your files to edge locations, but you don't have to pay for invalidating files.

Option B is incorrect because even though using invalidation will solve this issue, this solution is more expensive as compared to Option 1.

Option C is incorrect because configuring a separate cache behavior path having a custom object caching with a Minimum TTL of 0 alone is not enough to solve the problem. A cache behavior is primarily used to configure a variety of CloudFront functionality for a given URL path pattern for files on your website. Although this solution may work, it is still better to use versioned objects where you can control which image will be returned by the system even when the user has another version cached either locally or behind a corporate caching proxy.

Option D is incorrect because although it is right to configure your origin to add the Cache-Control or Expires header field, you should do this to your objects and not on the entire S3 bucket.

References:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/UpdatingExistingObjects.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/prevent-cloudfront-from-caching-files/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html#PayingForInvalidation>

[Go back to Q444](#)

Answer to Q445: B

[Go back to Q445](#)

Explanation to Q445

NA

[Go back to Q445](#)

Answer to Q446: C

[Go back to Q446](#)

Explanation to Q446

For this scenario, you can create a new Route 53 with the failover option to a static S3 website bucket or CloudFront distribution as an alternative.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/>

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

[Go back to Q446](#)

Answer to Q447: C

[Go back to Q447](#)

Explanation to Q447

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a group at launch time, the instance is automatically assigned to the default security group for the VPC. Changes made in a Security Group is immediately implemented.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

[Go back to Q447](#)

Answer to Q448: D

[Go back to Q448](#)

Explanation to Q448

Use the following best practices for monitoring to help you with your Amazon EC2 monitoring tasks. Make monitoring a priority to head off small problems before they become big ones. Create and implement a monitoring plan that collects monitoring data from all the parts in your AWS solution so that you can more easily debug a multi-point failure if one occurs.

Your monitoring plan should address, at a minimum, the following questions:

- What are your goals for monitoring?
- What resources will you monitor?
- How often will you monitor these resources?
- What monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something goes wrong? Automate monitoring tasks as much as possible. Check the log files on your EC2 instances.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_best_practices.html

[Go back to Q448](#)

Answer to Q449: B

[Go back to Q449](#)

Explanation to Q449

You can copy an Amazon Machine Image (AMI) within or across an AWS region using the AWS Management Console, the AWS command line tools or SDKs, or the Amazon EC2 API, all of which support the `CopyImage` action. You can copy both Amazon EBS-backed AMIs and instance store-backed AMIs. You can copy encrypted AMIs and AMIs with encrypted snapshots. Copying a source AMI results in an identical but distinct target AMI with its own unique identifier. In the case of an Amazon EBS-backed AMI, each of its backing snapshots is, by default, copied to an identical but distinct target snapshot. (The one exception is when you choose to encrypt the snapshot.) You can change or deregister the source AMI with no effect on the target AMI. The reverse is also true. There are no charges for copying an AMI. However, standard storage and data transfer rates apply.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>

[Go back to Q449](#)

Answer to Q450: D

[Go back to Q450](#)

Explanation to Q450

NA

[Go back to Q450](#)

Answer to Q451: E

[Go back to Q451](#)

Explanation to Q451

NA

[Go back to Q451](#)

Answer to Q452: C

[Go back to Q452](#)

Explanation to Q452

You can authenticate users in your organization's network and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate user name and password. This is known as the single sign-on (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory. You can also use SAML 2.0 to manage your own solution for federating user identities.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

[Go back to Q452](#)

Answer to Q453: C

[Go back to Q453](#)

Explanation to Q453

The important concept that you must understand in the scenario is that your VPC and your S3 bucket are located within the larger AWS network. However, the traffic coming from your VPC to your S3 bucket is traversing the public Internet by default. To better protect your data in transit, you can set up a VPC endpoint so the incoming traffic from your VPC will not pass through the public Internet, but instead through the private AWS network. A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

Traffic between your VPC and the other services do not leave the Amazon network. Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic. There are two types of VPC endpoints: interface endpoints and gateway endpoints. You should create the type of VPC endpoint required by the supported service. As a rule of thumb, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Option C is correct because VPC Endpoint Gateway supports private connection to S3.

Option A is incorrect because Internet gateway is used for instances in the public subnet to have accessibility to the Internet.

Option B is incorrect because VPC Interface Endpoint does not support the S3 service. You should use a VPC Endpoint Gateway instead. As mentioned in the above explanation, most AWS services use VPC Interface Endpoint except for S3 and DynamoDB, which use VPC Gateway Endpoint.

Option D is incorrect because NAT Gateway allows instances in the private subnet to gain access to the Internet, but not vice versa.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>

[Go back to Q453](#)

Answer to Q454: B

[Go back to Q454](#)

Explanation to Q454

Amazon Web Services (AWS) offers cloud storage services to support a wide range of storage workloads such as EFS, S3 and EBS. You must understand when you should use Amazon EFS, Amazon S3 and Amazon Elastic Block Store (EBS) based on the specific workloads. In this scenario, the keywords are rapidly changing data and 1000 Linux servers. Amazon EFS is a file storage service for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the same level of high availability and high scalability like S3 however, this service is more suitable for scenarios where it is required to have a POSIX-compatible file system or if you are storing rapidly changing data.

Data that must be updated very frequently might be better served by storage solutions that consider read and write latencies, such as Amazon EBS volumes, Amazon RDS, Amazon DynamoDB, Amazon EFS, or relational databases running on Amazon EC2. Amazon EBS is a block-level storage service for use with Amazon EC2. Amazon EBS can deliver performance for

workloads that require the lowest-latency access to data from a single EC2 instance. Amazon S3 is an object storage service. Amazon S3 makes data available through an Internet API that can be accessed anywhere.

In this scenario, Option B is the best answer. As stated above, Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances. EFS provides the performance, durability, high availability, and storage capacity needed by the 1000 Linux servers in the scenario.

Option A is incorrect because although S3 provides the same level of high availability and high scalability like EFS, this service is not suitable for storing data which are rapidly changing, just as mentioned in the above explanation. It is still more effective to use EFS as it offers strong consistency and file locking which the S3 service lacks.

Option C is incorrect because an EBS Volume cannot be shared by multiple instances.

Option D is incorrect because Storage Gateway is primarily used to extend the storage of your on-premises data center to your AWS Cloud.

References:

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

<https://aws.amazon.com/efs/features/>

<https://d1.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf#page=9>

[Go back to Q454](#)

Answer to Q455: C

[Go back to Q455](#)

Explanation to Q455

The default termination policy is designed to help ensure that your network architecture spans Availability Zones evenly.

With the default termination policy, the behavior of the Auto Scaling group is as follows:

1. If there are instances in multiple Availability Zones, choose the Availability Zone with the most instances and at least one instance that is not protected from scale in. If there is more than one Availability Zone with this number of instances, choose the Availability Zone with the instances that use the oldest launch configuration.
2. Determine which unprotected instances in the selected Availability Zone use the oldest launch configuration. If there is one such instance, terminate it.
3. If there are multiple instances to terminate based on the above criteria, determine which unprotected instances are closest to the next billing hour.

(This helps you maximize the use of your EC2 instances and manage your Amazon EC2 usage costs.) If there is one such instance, terminate it.

4. If there is more than one unprotected instance closest to the next billing hour, choose one of these instances at random. The following flow diagram illustrates how the default termination policy works:

Reference:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-termination-policy>

[Go back to Q455](#)

Answer to Q456: D

[Go back to Q456](#)

Explanation to Q456

By default, your instance is enabled for basic monitoring. You can optionally enable detailed monitoring. After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance. The following table describes basic and detailed monitoring for instances. Basic - Data is available automatically in 5-minute periods at no charge. Detailed - Data is available in 1-minute periods for an additional cost. To get this level of data, you must specifically enable it for the instance. For the instances where you've enabled detailed monitoring, you can also get aggregated data across groups of similar instances.

References:

<https://aws.amazon.com/cloudwatch/faqs/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html>

[Go back to Q456](#)

Answer to Q457: B

[Go back to Q457](#)

Explanation to Q457

Amazon Elastic File System (Amazon EFS) provides simple, scalable, elastic file storage for use with AWS Cloud services and on-premises resources. When mounted on Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics, allowing you to seamlessly integrate Amazon EFS with your existing

applications and tools. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, allowing Amazon EFS to provide a common data source for workloads and applications running on more than one Amazon EC2 instance. This scenario tests your understanding of EBS, EFS, and S3. In this scenario, there is a fleet of On-Demand EC2 instances that stores file documents from the users to one of the attached EBS Volumes. The system performance is quite slow because the architecture doesn't provide the EC2 instances a parallel shared access to the file documents. Remember that an EBS Volume can be attached to one EC2 instance at a time, hence, no other EC2 instance can connect to that EBS Provisioned IOPS Volume. Take note as well that the type of storage needed here is a "file storage" which means that S3 (Option A) is not the best service to use because it is mainly used for "object storage", and S3 does not provide the notion of "folders" too.

Therefore Option B is the correct answer.

Option C is incorrect because the scenario requires you to set up a scalable, high throughput storage system that will allow concurrent access from multiple EC2 instances. This is clearly not possible in EBS, even with Provisioned IOPS SSD Volumes. You must use EFS instead.

Option D is incorrect because ElastiCache is an in-memory data store that improves the performance of your applications, which is not what you need since it is not a file storage.

Reference:

<https://aws.amazon.com/efs/>

[Go back to Q457](#)

Answer to Q458: B

[Go back to Q458](#)

Explanation to Q458

NA

[Go back to Q458](#)

Answer to Q459: A

[Go back to Q459](#)

Explanation to Q459

Amazon EC2 has a soft limit of 20 instances per region, which can be easily resolved by completing the Amazon EC2 instance request form where your use case and your instance increase will be considered. Limit increases are tied to the region they were requested for.

Option B is incorrect as there is no such limit in the Availability Zone.

Option C is incorrect. Network Access List is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. It does not affect the creation of new EC2 instances.

Option D is incorrect as there is no problem with your API credentials.

References:

https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2

http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

[Go back to Q459](#)

Answer to Q460: C

[Go back to Q460](#)

Explanation to Q460

NA

[Go back to Q460](#)

Answer to Q461: B, E

[Go back to Q461](#)

Explanation to Q461

In this scenario, you have two VPCs which have peering connections with each other. Note that a VPC peering connection does not support edge to edge routing.

This means that if either VPC in a peering relationship has one of the following connections, you cannot extend the peering relationship to that connection:

- A VPN connection or an AWS Direct Connect connection to a corporate network
- An internet connection through an internet gateway
- An internet connection in a private subnet through a NAT device
- A VPC endpoint to an AWS service; for example, an endpoint to Amazon S3.
- (IPv6) A ClassicLink connection. You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection.

However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication. For example, if VPC A and VPC B are peered, and VPC A has any of these connections, then instances in VPC B cannot use the connection to access resources on the other side of the connection. Similarly, resources on the other side of a connection cannot use the connection to access VPC B. Hence, this means that you cannot use

VPC-2 to extend the peering relationship that exists between VPC-1 and the on-premise network. For example, traffic from the corporate network can't directly access VPC-1 by using the VPN connection or the AWS Direct Connect connection to VPC-2, which is why Options 1, 3, and 4 are incorrect. The correct answers are options 2 and 5.

You can do the following to provide a highly available, fault-tolerant network connection:

- Establish a hardware VPN over the Internet between the VPC and the on-premises network
- Establish another AWS Direct Connect connection and private virtual interface in the same AWS region

References:

<https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-to-edge-vgw>

<https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/>

<https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/>

[Go back to Q461](#)

Answer to Q462: A, C

[Go back to Q462](#)

Explanation to Q462

Amazon EBS encryption offers seamless encryption of EBS data volumes, boot volumes, and snapshots, eliminating the need to build and maintain a secure key management infrastructure. EBS encryption enables data at rest

security by encrypting your data using Amazon-managed keys, or keys you create and manage using the AWS Key Management Service (KMS). The encryption occurs on the servers that host EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.

Hence, options A and C are the right answers.

Options B and D are incorrect as these relate only to S3.

Option E is incorrect as you only store keys in CloudHSM and not passwords.

Option F is incorrect as ACM only provides SSL certificates and not data encryption of EBS Volumes.

Reference:

<https://aws.amazon.com/ebs/faqs/>

[Go back to Q462](#)

Answer to Q463: D

[Go back to Q463](#)

Explanation to Q463

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache that can reduce Amazon DynamoDB response times from milliseconds to microseconds, even at millions of requests per second.

Option A is incorrect because the Amazon Elasticsearch service is a fully managed service that makes it easy for you to deploy, secure, operate, and scale your Elasticsearch engine to search, analyze, and visualize data in real-time. Although you may integrate Elasticsearch with DynamoDB, it will not reduce the DynamoDB response time from milliseconds to

microseconds, even at millions of requests per second, whereas DynamoDB DAX can.

Option B is incorrect because AWS Device Farm is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time.

Option C is incorrect because DynamoDB Auto Scaling is primarily used to automate capacity management for your tables and global secondary indexes.

References:

<https://aws.amazon.com/dynamodb/dax>

<https://aws.amazon.com/device-farm>

[Go back to Q463](#)

Answer to Q464: C

[Go back to Q464](#)

Explanation to Q464

Scaling based on a schedule allows you to scale your application in response to predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the predictable traffic patterns of your web application.

To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled

scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action.

At the specified time, Amazon EC2 Auto Scaling updates the group with the values for minimum, maximum, and desired size specified by the scaling action. You can create scheduled actions for scaling one time only or for scaling on a recurring schedule.

Option C is the correct answer. You need to configure a Scheduled scaling policy. This will ensure that the instances are already scaled up and ready before the start of the day since this is when the application is used the most.

Options A and B are incorrect because although this is a valid solution, it is still better to configure a Scheduled scaling policy as you already know the exact peak hours of your application. By the time either the CPU or Memory hits a peak, the application already has performance issues, so you need to ensure the scaling is done beforehand using a Scheduled scaling policy.

Option D is incorrect. Although the Application load balancer can also balance the traffic, it cannot increase the instances based on demand.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

[Go back to Q464](#)

Answer to Q465: D

[Go back to Q465](#)

Explanation to Q465

All of these happen when you stop a running EBS-backed EC2 instance except for Option D. The instance retains its associated Elastic IP addresses if it is in the EC2-VPC platform and not on EC2-Classic.

When you stop a running instance, the following happens:

- The instance performs a normal shutdown and stops running; its status changes to stopping and then stopped.
- Any Amazon EBS volume remains attached to the instance, and their data persists. -Any data stored in the RAM of the host computer or the instance store volumes of the host computer are gone.
- In most cases, the instance is migrated to a new underlying host computer when it's started.
- EC2-Classic: AWS releases the public and private IPv4 addresses for the instance when you stop the instance and assign new ones when you restart it.
- EC2-VPC: The instance retains its private IPv4 addresses and any IPv6 addresses when stop and restart. AWS releases the public IPv4 address and assigns a new one when you restart it.
- EC2-Classic: AWS disassociates any Elastic IP address that's associated with the instance. You're charged for Elastic IP addresses that aren't associated with an instance. When you restart the instance, you must associate the Elastic IP address with the instance; AWS doesn't do this automatically.
- EC2-VPC: The instance retains its associated Elastic IP addresses. You're charged for any Elastic IP addresses associated with a stopped instance

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html

[Go back to Q465](#)

Answer to Q466: B

[Go back to Q466](#)

Explanation to Q466

Always remember that the messages in the SQS queue will continue to exist even after the EC2 instance has processed it, until you delete that message. You must ensure that you delete the message after processing to prevent the message from being received and processed again once the visibility timeout expires. There are three main parts in a distributed messaging system:

1. The components of your distributed system (EC2 instances)
2. Your queue (distributed on Amazon SQS servers)
3. Messages in the queue. You can set up a system which has several components that send messages to the queue and receive messages from the queue. The queue redundantly stores the messages across multiple Amazon SQS servers.

Refer to the third step of the SQS Message Lifecycle: Component 1 sends Message A to a queue, and the message is distributed across the Amazon SQS servers redundantly. When Component 2 is ready to process a message, it consumes messages from the queue, and Message A is returned. While Message A is being processed, it remains in the queue and isn't returned to subsequent receive requests for the duration of the visibility timeout. Component 2 deletes Message A from the queue to prevent the message from being received and processed again once the visibility timeout expires.

References:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-architecture.html>

[Go back to Q466](#)

Answer to Q467: B

[Go back to Q467](#)

[Explanation to Q467](#)

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported. Throughput Optimized HDD (st1) volumes, though like Cold HDD (sc1) volumes, are designed to support frequently accessed data.

Option A is incorrect because Amazon EBS Provisioned IOPS SSD is not the most cost-effective EBS type and is primarily used for critical business applications that require sustained IOPS performance.

Option C is incorrect because although an Amazon EBS General Purpose SSD volume balances price and performance for a wide variety of workloads, it is not suitable for frequently accessed, throughput-intensive workloads. Throughput Optimized HDD is a more suitable option to use than General Purpose SSD.

Option D is incorrect because although Amazon EBS Cold HDD provides the lowest cost HDD volume compared to General Purpose SSD, it is much suitable for less frequently accessed workloads.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_st1

[Go back to Q467](#)

Answer to Q468: B

[Go back to Q468](#)

Explanation to Q468

NA

[Go back to Q468](#)

Answer to Q469: C

[Go back to Q469](#)

Explanation to Q469

AWS offers two kinds of NAT devices a NAT gateway or a NAT instance. It is recommended to use NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI. Just like a NAT instance, you can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. Here is a diagram showing the differences between NAT gateway and NAT instance:

Option A is incorrect because an Egress-only Internet gateway is primarily used for VPCs that use IPv6 to enable instances in a private subnet to

connect to the Internet or other AWS services, but prevent the Internet from initiating a connection with those instances, just like what NAT Instance and NAT Gateway do. The scenario explicitly says that the EC2 instances are using IPv4 addresses which is why Egress-only Internet gateway is invalid, even though it can provide the required high availability.

Option B is incorrect because a VPC endpoint simply enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Option D is incorrect because although a NAT instance can also enable instances in a private subnet to connect to the Internet or other AWS services and prevent the Internet from initiating a connection with those instances, it is not as highly available compared to a NAT Gateway.

References:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

[Go back to Q469](#)

Answer to Q470: A

[Go back to Q470](#)

[Explanation to Q470](#)

NA

[Go back to Q470](#)

Answer to Q471: C

[Go back to Q471](#)

Explanation to Q471

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

Option A is incorrect because DynamoDB is primarily used as a NoSQL database which supports both document and key-value store models. ElastiCache is a more suitable service to use than DynamoDB, if you need an in-memory data store.

Option B is incorrect because RDS is mainly used as a relational database and not as a data storage for frequently used data.

Option D is incorrect because Redshift is a data warehouse service and is not suitable to be used as an in-memory data store.

References:

<https://aws.amazon.com/elasticache/>

<https://aws.amazon.com/products/databases/>

[Go back to Q471](#)

Answer to Q472: D

[Go back to Q472](#)

Explanation to Q472

In this scenario, the load balancer will route the incoming requests only to the healthy instances. When the load balancer determines that an instance is unhealthy, it stops routing requests to that instance. The load balancer resumes routing requests to the instance when it has been restored to a healthy state.

There are two ways of checking the status of your EC2 instances:

1. Via the Auto Scaling group
2. Via the ELB health checks

The default health checks for an Auto Scaling group are EC2 status checks only. If an instance fails these status checks, the Auto Scaling group considers the instance unhealthy and replaces. If you attached one or more load balancers or target groups to your Auto Scaling group, the group does not, by default, consider an instance unhealthy and replace it if it fails the load balancer health checks. However, you can optionally configure the Auto Scaling group to use Elastic Load Balancing health checks. This ensures that the group can determine an instance's health based on additional tests provided by the load balancer. The load balancer periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. If you configure the Auto Scaling group to use Elastic Load Balancing health checks, it considers the instance unhealthy if it fails either the EC2 status checks or the load balancer health checks. If you attach multiple load balancers to an Auto Scaling group, all of them must report that the instance is healthy for it to consider the instance healthy. If one load balancer reports an instance as unhealthy, the Auto Scaling group replaces the instance, even if other load balancers report it as healthy.

References:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html>

[Go back to Q472](#)

Answer to Q473: B, C

[Go back to Q473](#)

Explanation to Q473

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. Amazon Glacier is designed to store data that is infrequently accessed. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

Option A is incorrect because storing cached session data is the main use case for ElastiCache and not Amazon Glacier.

Option D is incorrect because you should use RDS or DynamoDB for your active database storage as S3, in general, is used for storing your data or files.

Option E is incorrect because storing it for data warehousing is the main use case of Amazon Redshift. It does not meet the requirement of being able to archive your infrequently accessed data. You can use S3 standard instead for frequently accessed data or Glacier for infrequently accessed data and archiving. It is advisable to transition the standard data to infrequent access first then transition it to Amazon Glacier. You can specify

in the lifecycle rule the time it will sit in standard tier and infrequent access. You can also delete the objects after a certain amount of time.

In transitioning S3 standard to Glacier you need to tell S3 which objects are to be archived to the new Glacier storage option, and under what conditions.

You do this by setting up a lifecycle rule using the following elements:

- A prefix to specify which objects in the bucket are subject to the policy.
- A relative or absolute time specifier and a time period for transitioning objects to Glacier. The time periods are interpreted with respect to the object's creation date. They can be relative (migrate items that are older than a certain number of days) or absolute (migrate items on a specific date)
- An object age at which the object will be deleted from S3. This is measured from the original PUT of the object into the service, and the clock is not reset by a transition to Glacier.

You can create a lifecycle rule in the AWS Management Console.

Reference:

<https://aws.amazon.com/glacier/faqs/>

[Go back to Q473](#)

Answer to Q474: A, B

[Go back to Q474](#)

Explanation to Q474

NA

[Go back to Q474](#)

Answer to Q475: C

[Go back to Q475](#)

Explanation to Q475

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you're already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

Options A and B are incorrect because Amazon S3 Select is just a feature of Amazon S3. Likewise, Redshift Spectrum is also just a feature of Amazon Redshift. Although Amazon Kinesis Data Firehose can load streaming data to both Amazon S3 and Amazon Redshift, it does not directly load the data to S3 Select and Redshift Spectrum. S3 Select is an Amazon S3 feature that makes it easy to retrieve specific data from the contents of an object using simple SQL expressions without having to retrieve the entire object.

Amazon Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of unstructured data in Amazon S3 with no loading or ETL required.

Option D is incorrect because Amazon Kinesis Data Firehose cannot load streaming data to Athena.

Reference:

<https://aws.amazon.com/kinesis/data-firehose/>

[Go back to Q475](#)

Answer to Q476: D

[Go back to Q476](#)

Explanation to Q476

When you create or update Lambda functions that use environment variables, AWS Lambda encrypts them using the AWS Key Management Service. When your Lambda function is invoked, those values are decrypted and made available to the Lambda code. The first time you create or update Lambda functions that use environment variables in a region, a default service key is created for you automatically within AWS KMS. This key is used to encrypt environment variables.

However, if you wish to use encryption helpers and use KMS to encrypt environment variables after your Lambda function is created, you must create your own AWS KMS key and choose it instead of the default key. The default key will give errors when chosen. Creating your own key gives you more flexibility, including the ability to create, rotate, disable, and define access controls, and to audit the encryption keys used to protect your data.

Reference:

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html#env_encrypt

[Go back to Q476](#)

Answer to Q477: A

[Go back to Q477](#)

Explanation to Q477

To calculate the total number of IP addresses of a given CIDR Block, you simply need to follow the 2 easy steps below. Let's say you have a CIDR block /27: 1. Subtract 32 with the mask number : $(32 - 27) = 5$ 2. Raise the number 2 to the power of the answer in Step #1 : $2^5 = (2 * 2 * 2 * 2 * 2) = 32$ The answer to Step #2 is the total number of IP addresses available in the given CIDR netmask. Don't forget that in AWS, the first 4 IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance.

In addition, you can always associate a netmask of /27 which also has the same number of usable IP addresses (27) to help you with your exam.

Option A is the correct answer because the CIDR block of 172.0.0.0/27, with a netmask of /27, has an equivalent of 27 usable IP addresses. Take note that a netmask of /27 originally provides you with 32 IP addresses but in AWS, there are 5 IP addresses that are reserved which you cannot use. The first 4 IP addresses and the last IP address in each subnet CIDR block are not available in your VPC which means that you must always subtract 5 IP addresses, hence $32 - 5 = 27$.

Option B is incorrect as a netmask of /28 only supports 16 IP Addresses.

Options C and D are incorrect as the only allowed block size is between a /28 netmask and /16 netmask.

To add a CIDR block to your VPC, the following rules apply:

- The allowed block size is between a /28 netmask and /16 netmask.
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
- You cannot increase or decrease the size of an existing CIDR block.

- You have a limit on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your limits.
- The CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables.

For example, if you have a route with a destination of 10.0.0.0/24 to a virtual private gateway, you cannot associate a CIDR block of the same range or larger. However, you can associate a CIDR block of 10.0.0.0/25 or smaller.

- The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

[Go back to Q477](#)

Answer to Q478: A

[Go back to Q478](#)

Explanation to Q478

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop and Apache Spark, on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large

amounts of data into and out of other AWS data stores and databases such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.

Option B is wrong as Amazon Glacier is used for data archive only.

Option C is wrong as an EC2 instance is not a recommended storage service. In addition, Amazon EC2 does not have a built-in data processing engine to process large amounts of data.

Option D is wrong as Amazon RedShift is mainly used as a data warehouse service.

Reference:

<http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

[Go back to Q478](#)

Answer to Q479: A, B

[Go back to Q479](#)

Explanation to Q479

You can connect and manage the EC2 instance, so Option B is correct. You can install new packages and perform changes on the underlying infrastructure of the EC2 instance such as Enhanced Networking, Encryption, and so forth. Elastic Beanstalk is a service that allows you to quickly deploy and manage your application in AWS.

What it does is to automatically create EC2 instances for your application, which you can also manage just like a regular instance.

Hence, Option A is correct.

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

[Go back to Q479](#)

Answer to Q480: D

[Go back to Q480](#)

Explanation to Q480

NA

[Go back to Q480](#)

Answer to Q481: C

[Go back to Q481](#)

Explanation to Q481

NA

[Go back to Q481](#)

Answer to Q482: A, B

[Go back to Q482](#)

Explanation to Q482

Here are the prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:

- An S3 bucket that is configured to host a static website. The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain acme.example.com, the name of the bucket must be acme.example.com.
- A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.
- Route 53 as the DNS service for the domain. If you register your domain name by using Route 53, we automatically configure Route 53 as the DNS service for the domain.

Reference:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html>

[Go back to Q482](#)

Answer to Q483: B

[Go back to Q483](#)

Explanation to Q483

NA

[Go back to Q483](#)

Answer to Q484: C, E

[Go back to Q484](#)

Explanation to Q484

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a front door for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application. Since it can use AWS Lambda, you can run your APIs without servers. Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive, and the amount of data transferred out.

Reference:

<https://aws.amazon.com/api-gateway/>

[Go back to Q484](#)

Answer to Q485: D

[Go back to Q485](#)

Explanation to Q485

NA

[Go back to Q485](#)

Answer to Q486: A

[Go back to Q486](#)

Explanation to Q486

Since you need to connect to your EC2 instance via the Internet, you basically need to ensure that your VPC has an attached Internet Gateway so it can communicate with the outside world. Your instance should also have either public IP or Elastic IP address. In this scenario, you don't need a Secondary Private IP Address since it is only used inside your VPC.

To enable access to or from the internet for instances in a VPC subnet, you must do the following:

- Attach an internet gateway to your VPC.
- Ensure that your subnet's route table points to the internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

References:

<https://aws.amazon.com/premiumsupport/knowledge-center/secondary-private-ip-address/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html/>

[Go back to Q486](#)

Answer to Q487: C

[Go back to Q487](#)

Explanation to Q487

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to

run ad-hoc queries and get results in seconds. Athena is serverless, so there is no infrastructure to set up or manage, and you pay only for the queries you run. Athena scales automatically executing queries in parallel, so results are fast, even with large datasets and complex queries. Athena helps you analyze unstructured, semi-structured, and structured data stored in Amazon S3. Examples include CSV, JSON, or columnar data formats such as Apache Parquet and Apache ORC. You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena.

Hence, the most cost-effective and appropriate answer in this scenario is Option C: Using AWS Athena.

Options A, B and D are all incorrect because it is not necessary to set up a database to be able to analyze the CSV export file. You can use a cost-effective option (AWS Athena), which is a serverless service that enables you to pay only for the queries you run.

Reference:

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

[Go back to Q487](#)

Answer to Q488: B

[Go back to Q488](#)

Explanation to Q488

Failover is automatically handled by Amazon Aurora so that your applications can resume database operations as quickly as possible without manual administrative intervention. If you have an Amazon Aurora Replica in the same or a different Availability Zone, when failing over, 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. Start-to-finish, failover typically completes within 30 seconds.

If you do not have an Amazon Aurora Replica (i.e. single instance), Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone. From start to finish, failover typically completes in under 15 minutes.

Hence, the correct answer is Option B.

Options A and C are incorrect because this will only happen if you are using an Amazon Aurora Replica. In addition, Amazon Aurora flips the canonical name record (CNAME) and not the A record (IP address) of the instance.

Option D is incorrect because Aurora will first attempt to create a new DB Instance in the same Availability Zone as the original instance. If unable to do so, Aurora will attempt to create a new DB Instance in a different Availability Zone and not the other way around.

Reference:

<https://aws.amazon.com/rds/aurora/faqs/>

[Go back to Q488](#)

Answer to Q489: C, D

[Go back to Q489](#)

Explanation to Q489

In Auto Scaling, the following statements are correct regarding the cooldown period: It ensures that the Auto Scaling group does not launch or terminate additional EC2 instances before the previous scaling activity

takes effect. Its default value is 300 seconds. It is a configurable setting for your Auto Scaling group.

Options A, B, and E are incorrect as these statements are false in depicting what the word "cooldown" means for Auto Scaling. The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect.

After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities.

Reference:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-termination.html>

[Go back to Q489](#)

Answer to Q490: C, D

[Go back to Q490](#)

Explanation to Q490

NA

[Go back to Q490](#)

Answer to Q491: C

[Go back to Q491](#)

Explanation to Q491

The virtual devices for instance store volumes are named as ephemeral[0-23]. Instance types that support one instance store volume have ephemeral0. Instance types that support two instance store volumes have ephemeral0 and ephemeral1, and so on until ephemeral23. The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists.

However, data in the instance store is lost under the following circumstances:

- The underlying disk drive fails
- The instance stops
- The instance terminates

The word ephemeral means short-lived or temporary in the English dictionary. Hence, when you see this word in AWS, always consider this as just a temporary memory or a short-lived storage.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html?shortFooter=true#instance-store-lifetime>

[Go back to Q491](#)

Answer to Q492: D

[Go back to Q492](#)

Explanation to Q492

NA

[Go back to Q492](#)

Answer to Q493: A

[Go back to Q493](#)

Explanation to Q493

There is no additional charge for AWS CloudFormation. You only pay for the AWS resources that are created (e.g. Amazon EC2 instances, Elastic Load Balancing load balancers, etc.)

Reference:

<https://aws.amazon.com/cloudformation/faqs/>

[Go back to Q493](#)

Answer to Q494: A

[Go back to Q494](#)

Explanation to Q494

When you create or modify your DB instance to run as a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone.

Updates to your DB Instance are synchronously replicated across Availability Zones to the standby in order to keep both in sync and protect your latest database updates against DB instance failure.

Option B is incorrect as a Read Replica provides an asynchronous replication instead of synchronous.

In addition, a Read Replica is only available in Aurora, MySQL, MariaDB, and PostgreSQL database engines.

Options C and D are wrong answers as both DynamoDB and CloudFront do not have a Read Replica feature.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q494](#)

Answer to Q495: C

[Go back to Q495](#)

Explanation to Q495

In Amazon Redshift, you use workload management (WLM) to define the number of query queues that are available, and how queries are routed to those queues for processing. WLM is part of parameter group configuration. A cluster uses the WLM configuration that is specified in its associated parameter group.

When you create a parameter group, the default WLM configuration contains one queue that can run up to five queries concurrently. You can add additional queues and configure WLM properties in each of them if you want more control over query processing. Each queue that you add has the same default WLM configuration until you configure its properties.

When you add additional queues, the last queue in the configuration is the default queue. Unless a query is routed to another queue based on criteria in the WLM configuration, it is processed by the default queue. You cannot specify user groups or query groups for the default queue. As with other parameters, you cannot modify the WLM configuration in the default parameter group. Clusters associated with the default parameter group always use the default WLM configuration.

If you want to modify the WLM configuration, you must create a parameter group and then associate that parameter group with any clusters that require your custom WLM configuration.

Reference:

<https://docs.aws.amazon.com/redshift/latest/mgmt/workload-mgmt-config.html>

[Go back to Q495](#)

Answer to Q496: A

[Go back to Q496](#)

Explanation to Q496

In Amazon S3, all objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a pre-signed URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The pre-signed URLs are valid only for the specified duration. Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

Reference:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

[Go back to Q496](#)

Answer to Q497: A, E

[Go back to Q497](#)

Explanation to Q497

By using Versioning and enabling MFA (Multi-Factor Authentication) Delete, you can secure and recover your S3 objects from accidental deletion or overwrite.

Versioning is a means of keeping multiple variants of an object in the same bucket. Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. You can also optionally add another layer of security by configuring a bucket to enable MFA (Multi-Factor Authentication) Delete, which requires additional authentication for either of the following operations: Change the versioning state of your bucket Permanently delete an object version.

MFA Delete requires two forms of authentication together: Your security credentials.

The concatenation of a valid serial number, a space, and the six-digit code displayed on an approved authentication device.

Reference:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

[Go back to Q497](#)

Answer to Q498: B, D

[Go back to Q498](#)

Explanation to Q498

The question refers to one of the common scenarios for temporary credentials in AWS. Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles.

In this example, it is called enterprise identity federation considering that you also need to set up a single sign-on (SSO) capability. The correct answers are:

- Setup a Federation proxy or an Identity provider
- Setup an AWS Security Token Service to generate temporary tokens
- Configure an IAM role

In an enterprise identity federation, you can authenticate users in your organization's network, and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate user name and password. This is known as the single sign-on (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory. You can also use SAML 2.0 to manage your own solution for federating user identities.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

[Go back to Q498](#)

Answer to Q499: C

[Go back to Q499](#)

Explanation to Q499

The main issue here is that the order management system produces duplicate orders at times. Since the company is using SQS, there is a possibility that a message can have a duplicate in case an EC2 instance failed to delete the already processed message. To prevent this issue from happening, you must use Amazon Simple Workflow service instead of SQS. For standard queues, the visibility timeout isn't a guarantee against receiving a message twice.

Hence, Option B is incorrect. To avoid duplicate SQS messages, it is better to design your applications to be idempotent (they should not be affected adversely when processing the same message more than once). Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps.

You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the Cloud. If your app's steps take more than 500 milliseconds to complete, you need to track the state of processing, and you need to recover or retry if a task fails.

References:

<https://aws.amazon.com/swf/>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

[Go back to Q499](#)

Answer to Q500: A

[Go back to Q500](#)

Explanation to Q500

NA

[Go back to Q500](#)

Answer to Q501: B

[Go back to Q501](#)

Explanation to Q501

Since the web portal consists of both web and database servers, it is best to launch the web servers into the public subnet and the database server into the private subnet. Hence, Option B is the right answer. Although you can use a single public subnet for your web and database servers, it will be a massive security risk as you are exposing your database publicly to the Internet.

Reference:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario_2.html

[Go back to Q501](#)

Answer to Q502: A, B

[Go back to Q502](#)

Explanation to Q502

NA

[Go back to Q502](#)

Answer to Q503: D

[Go back to Q503](#)

Explanation to Q503

Amazon Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet.

Reference:

<https://aws.amazon.com/snowball/>

[Go back to Q503](#)

Answer to Q504: C

[Go back to Q504](#)

Explanation to Q504

Instance metadata is the data about your instance that you can use to configure or manage the running instance. You can get the instance ID, public keys, public IP address and many other information from the instance metadata by firing a URL command in your instance to this URL:
<http://169.254.169.254/latest/meta-data/>

Option A is incorrect because the instance user data is mainly used to perform common automated configuration tasks and run scripts after the instance starts.

Option B is incorrect because resource tags are labels that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.

Option D is incorrect because Amazon Machine Image (AMI) mainly provides the information required to launch an instance, which is a virtual server in the cloud.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

[Go back to Q504](#)

Answer to Q505: C

[Go back to Q505](#)

Explanation to Q505

NA

[Go back to Q505](#)

Answer to Q506: C

[Go back to Q506](#)

Explanation to Q506

In this scenario, the best option is to use Amazon S3.

It's a simple storage service that offers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.

Options A and D are incorrect because these services do not provide durable storage.

Option B is incorrect because Amazon Glacier is mainly used for data archives with data retrieval times that can take some few hours.

Hence, it is not suitable for the transcription service where the data are stored and frequently accessed.

Reference:

<https://aws.amazon.com/s3/faqs/>

[Go back to Q506](#)

Answer to Q507: C

[Go back to Q507](#)

Explanation to Q507

The first step is to create a snapshot of the EBS volume. Create a volume using this snapshot and then specify the new Availability Zone accordingly.

A point-in-time snapshot of an EBS volume, can be used as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the entire volume. Snapshots occur asynchronously; the point-in-time snapshot is created immediately, but the status of the snapshot is pending until the snapshot is complete (when all of the modified blocks have been transferred to Amazon S3), which can take several hours for large initial snapshots or subsequent snapshots where many blocks have

changed. While it is completing, an in-progress snapshot is not affected by ongoing reads and writes to the volume.

References:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html>

[Go back to Q507](#)

Answer to Q508: A, D

[Go back to Q508](#)

Explanation to Q508

Considering that the company is using a corporate Active Directory, it is best to use AWS Directory Service AD Connector for easier integration. In addition, since the roles are already assigned using groups in the corporate Active Directory, it would be better to also use IAM Roles. Take note that you can assign an IAM Role to the users or groups from your Active Directory once it is integrated with your VPC via the AWS Directory Service AD Connector.

AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory (AD) with other AWS services. Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources. AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)aware applications in the cloud.

It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

Reference:

<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

[Go back to Q508](#)

Answer to Q509: A, D

[Go back to Q509](#)

Explanation to Q509

Amazon SNS supports notifications over multiple transport protocols for customers to have broad flexibility of delivery mechanisms.

Customers can select one the following transports as part of the subscription requests:

- HTTP, HTTPS Subscribers specify a URL as part of the subscription registration; notifications will be delivered through an HTTP POST to the specified URL.
- Email, Email-JSON Messages are sent to registered addresses as email. Email-JSON sends notifications as a JSON object, while Email sends text-based email.
- SQS Users can specify an SQS standard queue as the endpoint; Amazon SNS will enqueue a notification message to the specified queue (which subscribers can then process using SQS APIs such as ReceiveMessage, DeleteMessage, etc.). Note that FIFO queues are not currently supported.

- SMS Messages are sent to registered phone numbers as SMS text messages.

Reference:

<https://aws.amazon.com/sns/faqs/>

[Go back to Q509](#)

Answer to Q510: D

[Go back to Q510](#)

Explanation to Q510

You can choose the credentials that are right for your IAM user. When you use the AWS Management Console to create a user, you must choose to at least include a console password or access keys. By default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. You must create the type of credentials for an IAM user based on the needs of your user.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services.

To fill this need, you can create, modify, view, or rotate access keys (access key IDs and secret access keys) for IAM users. When you create an access key, IAM returns the access key ID and secret access key. You should save these in a secure location and give them to the user.

Option A is incorrect because by default, a brand new IAM user created using the AWS CLI or AWS API has no credentials of any kind. Take note that in the scenario, you created the new IAM user using the AWS CLI and not via the AWS Management Console, where you must choose to at least include a console password or access keys when creating a new IAM user.

Option B is incorrect because enabling Multi-Factor Authentication for the IAM user will still not provide the required Access Keys needed to send API calls to your AWS resources. You must grant the IAM user with Access Keys to meet the requirement.

Option C is incorrect because adding a new IAM policy to the new user will not grant the needed Access Keys needed to make API calls to the AWS resources.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html#id_users_creds

[Go back to Q510](#)

Answer to Q511: A, C

[Go back to Q511](#)

Explanation to Q511

Amazon S3 Standard - Infrequent Access (Standard - IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. Standard - IA offers the high durability, throughput,

and low latency of Amazon S3 Standard, with a low per GB storage price and per GB retrieval fee.

This combination of low cost and high performance make Standard - IA ideal for long-term storage, backups, and as a data store for disaster recovery. The Standard - IA storage class is set at the object level and can exist in the same bucket as Standard, allowing you to use lifecycle policies to automatically transition objects between storage classes without any application changes.

Key Features:

- Same low latency and high throughput performance of Standard
- Designed for durability of 99.999999999% of objects
- Designed for 99.9% availability over a given year
- Backed with the Amazon S3 Service Level Agreement for availability
- Supports SSL encryption of data in transit and at rest
- Lifecycle management for automatic migration of objects

The option: "It provides high latency and low throughput performance" is wrong as it should be "low latency" and "high throughput" instead.

The option: "It is the best storage option to store noncritical and reproducible data" is wrong as it refers to Amazon S3 - Reduced Redundancy Storage (RRS).

The option: "Ideal to use for data archiving." is wrong because this statement refers to Amazon Glacier.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

[Go back to Q511](#)

Answer to Q512: A, D

[Go back to Q512](#)

Explanation to Q512

The correct answers are options A & D: Increased database availability in the case of system upgrades like OS patching or DB Instance scaling. It makes the database fault-tolerant to an Availability Zone failure.

Option C is almost correct. RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ) that is in the same region and not in a different one.

Options B and E are incorrect as it does not affect the performance nor provide SQL optimization. Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads.

When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.

Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

Reference:

<https://aws.amazon.com/rds/details/multi-az/>

[Go back to Q512](#)

Answer to Q513: B

[Go back to Q513](#)

Explanation to Q513

In an ideal and secure VPC architecture, you launch the web servers or elastic load balancers in the public subnet and the database servers in the private subnet. If you launch your database server in the public subnet, it will be publicly accessible all over the Internet which has a higher security risk. Hence, it is better to launch your database in the private subnet.

Reference:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

[Go back to Q513](#)

Answer to Q514: B

[Go back to Q514](#)

Explanation to Q514

To avoid accidental deletion in Amazon S3 bucket, you can:

- Enable Versioning
- Enable MFA (Multi-Factor Authentication) Delete Versioning is a means of keeping multiple variants of an object in the same bucket

You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

If the MFA (Multi-Factor Authentication) Delete is enabled, it requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

Reference:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

[Go back to Q514](#)

Answer to Q515: A, D

[Go back to Q515](#)

Explanation to Q515

NA

[Go back to Q515](#)

Answer to Q516: A

[Go back to Q516](#)

Explanation to Q516

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Building applications from individual components that each perform a discrete function improves scalability and reliability and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application.

Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available.

Reference:

<https://aws.amazon.com/sqs/>

[Go back to Q516](#)

Answer to Q517: A

[Go back to Q517](#)

Explanation to Q517

By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.

The key to managing sticky sessions is to determine how long your load balancer should consistently route the user's request to the same instance. If your application has its own session cookie, then you can configure Elastic Load Balancing so that the session cookie follows the duration specified.

If your application does not have its own session cookie, then you can configure Elastic Load Balancing to create a session cookie by specifying your own stickiness duration.

Reference:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-sticky-sessions.html>

[Go back to Q517](#)

Answer to Q518: A

[Go back to Q518](#)

Explanation to Q518

<http://169.254.169.254/latest/meta-data/> is the URL that you can use to retrieve the Instance Metadata of your EC2 instance, including the public-hostname, public-ipv4, public-keys et cetera. This can be helpful when you're writing scripts to run from your instance as it enables you to access the local IP address of your instance from the instance metadata to manage a connection to an external application.

Remember that you are not billed for HTTP requests used to retrieve instance metadata and user data.

Reference:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

[Go back to Q518](#)

Answer to Q519: C

[Go back to Q519](#)

Explanation to Q519

NA

[Go back to Q519](#)

Answer to Q520: C

[Go back to Q520](#)

Explanation to Q520

NA

[Go back to Q520](#)