질문 2: 오답

A streaming solutions company is building a video streaming product by using an Application Load Balancer (ALB) that routes the requests to the underlying EC2 instances. The engineering team has noticed a peculiar pattern. The ALB removes an instance from its pool of healthy instances whenever it is detected as unhealthy but the Auto Scaling group fails to kick-in and provision the replacement instance.

What could explain this anomaly?

설명 Correct option:

The Auto Scaling group is using EC2 based health check and the Application Load Balancer is using ALB based health check

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for automatic scaling and management.

Auto Scaling Group Overview: via - https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

Application Load Balancer automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.

If the Auto Scaling group (ASG) is using EC2 as the health check type and the Application Load Balancer (ALB) is using its in-built health check, there may be a situation where the ALB health check fails because the health check pings fail to receive a response from the instance. At the same time, ASG health check can come back as successful because it is based on EC2 based health check. Therefore, in this scenario, the ALB will remove the instance from its inventory, however, the ASG will fail to provide the replacement instance. This can lead to the scaling issues mentioned in the problem statement.

Incorrect options:

The Auto Scaling group is using ALB based health check and the Application Load Balancer is using EC2 based health check - ALB cannot use EC2 based health checks, so this option is incorrect.

Both the Auto Scaling group and Application Load Balancer are using ALB based health check - It is recommended to use ALB based health checks for both Auto Scaling group and Application Load Balancer. If both the Auto Scaling group and Application Load Balancer use ALB based health checks, then you will be able to avoid the scenario mentioned in the question.

Both the Auto Scaling group and Application Load Balancer are using EC2 based health check - ALB cannot use EC2 based health checks, so this option is incorrect.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html

질문 4: 정답

Reporters at a news agency upload/download video files (about 500MB each) to/from an S3 bucket as part of their daily work. As the agency has started offices in remote locations, it has resulted in poor latency for uploading and accessing data to/from the given S3 bucket. The agency wants to continue using a serverless storage solution such as S3 but wants to improve the performance.

As a solutions architect, which of the following solutions do you propose to address this issue? (Select two)

설명 Correct options:

Use Amazon CloudFront distribution with origin as the S3 bucket. This would speed up uploads as well as downloads for the video files

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, within a developer-friendly environment. When an object from S3 that is set up with CloudFront CDN is requested, the request would come through the Edge Location transfer paths only for the first request. Thereafter, it would be served from the nearest edge location to the users until it expires. So in this way, you can speed up uploads as well as downloads for the video files.

Following is a good reference blog for a deep-dive:

https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/

Enable Amazon S3 Transfer Acceleration for the S3 bucket. This would speed up uploads as well as downloads for the video files

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. Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. So this option is also correct.

Transfer Acceleration Overview: via - https://aws.amazon.com/s3/transfer-acceleration/

Incorrect options:

Create new S3 buckets in every region where the agency has a remote office, so that each office can maintain its storage for the media assets - Creating new S3 buckets in every region is not an option, since the agency maintains centralized storage. Hence this option is incorrect.

Move S3 data into EFS file system created in a US region, connect to EFS file system from EC2 instances in other AWS regions using an inter-region VPC peering connection

Spin up EC2 instances in each region where the agency has a remote office. Create a daily job to transfer S3 data into EBS volumes attached to the EC2 instances

Both these options using EC2 instances are not correct for the given use-case, as the agency wants a serverless storage solution.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

https://aws.amazon.com/s3/transfer-acceleration/

https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/

질문 6: 정답

A silicon valley based healthcare startup uses AWS Cloud for its IT infrastructure. The startup stores patient health records on Amazon S3. The engineering team needs to implement an archival solution based on Amazon S3 Glacier to enforce regulatory and compliance controls on data access.

As a solutions architect, which of the following solutions would you recommend?

설명 Correct option:

Use S3 Glacier vault to store the sensitive archived data and then use a vault lock policy to enforce compliance controls

Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 cloud storage class for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provide comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

An S3 Glacier vault is a container for storing archives. When you create a vault, you specify a vault name and the AWS Region in which you want to create the vault. S3 Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy. You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits. Therefore, this is the correct option.

Incorrect options:

Use S3 Glacier to store the sensitive archived data and then use an S3 lifecycle policy to enforce compliance controls - You can use lifecycle policy to define actions you want Amazon S3 to take during an object's lifetime. For example, use a lifecycle policy to transition objects to another storage class, archive them, or delete them after a specified period. It cannot be used to enforce compliance controls. Therefore, this option is incorrect.

Use S3 Glacier vault to store the sensitive archived data and then use an S3 Access Control List to enforce compliance controls - Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. It cannot be used to enforce compliance controls. Therefore, this option is incorrect.

Use S3 Glacier to store the sensitive archived data and then use an S3 Access Control List to enforce compliance controls - Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. It cannot be used to enforce compliance controls. Therefore, this option is incorrect.

References:

https://docs.aws.amazon.com/amazonglacier/latest/dev/working-with-vaults.html

https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock.html

https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-lifecycle.html

질문 7: 정답

You are a cloud architect at an IT company. The company has multiple enterprise customers that manage their own mobile apps that capture and send data to Amazon Kinesis Data Streams. They have been getting a ProvisionedThroughputExceededException exception. You have been contacted to help and upon analysis, you notice that messages are being sent one by one at a high rate.

Which of the following options will help with the exception while keeping costs at a minimum?

설명 Correct options:

Use batch messages

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The data collected is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more.

Kinesis Data Streams Overview: via - https://aws.amazon.com/kinesis/data-streams/

When a host needs to send many records per second (RPS) to Amazon Kinesis, simply calling the basic PutRecord API action in a loop is inadequate. To reduce overhead and increase throughput, the application must batch records and implement parallel HTTP requests. This will increase the efficiency overall and ensure you are optimally using the shards.

Incorrect options:

Use Exponential Backoff: While this may help in the short term, as soon as the request rate increases, you will see the ProvisionedThroughputExceededException exception again.

Increase the number of shards - Increasing shards could be a short term fix but will substantially increase the cost, so this option is ruled out.

Decrease the Stream retention duration - This operation may result in data loss and won't help with the exceptions, so this option is incorrect.

References:

https://aws.amazon.com/blogs/big-data/implementing-efficient-and-reliable-producers-with-the-amazon-kinesis-producer-library/

https://aws.amazon.com/kinesis/data-streams/

질문 8: 정답

A company's cloud architect has set up a solution that uses Route 53 to configure the DNS records for the primary website with the domain pointing to the Application Load Balancer (ALB). The company wants a solution where users will be directed to a static error page, configured as a backup, in case of unavailability of the primary website.

Which configuration will meet the company's requirements, while keeping the changes to a bare minimum?

설명 Correct option:

Set up a Route 53 active-passive type of failover routing policy. If Route 53 health check determines the ALB endpoint as unhealthy, the traffic will be diverted to a static error page, hosted on Amazon S3 bucket

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 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.

Incorrect options:

Set up a Route 53 active-active type of failover routing policy. If Route 53 health check determines the ALB endpoint as unhealthy, the traffic will be diverted to a static error page, hosted on Amazon S3 bucket - This option has been added as a distractor as there is no such thing as an active-active failover routing policy in Route 53. You can configure active-active failover using any routing policy (or combination of routing policies) other than failover routing policy and you configure active-passive failover only using the failover routing policy. In active-active failover configuration, 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.

Use Route 53 Latency-based routing. Create a latency record to point to the Amazon S3 bucket that holds the error page to be displayed - 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 - this is Latency-based routing and is not helpful for the current use case.

Use Route 53 Weighted routing to give minimum weight to Amazon S3 bucket that holds the error page to be displayed. In case of primary failure, the requests get routed to the error page - 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 the software. This is not useful for the current use case.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html#dns-failover-types-active-passive

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency

질문 10: 정답

A company wants to ensure high availability for its RDS database. The development team wants to opt for Multi-AZ deployment and they would like to understand what happens when the primary instance of the Multi-AZ configuration goes down.

As a Solutions Architect, which of the following will you identify as the outcome of the scenario?

설명 Correct option:

The CNAME record will be updated to point to the standby DB - 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 MariaDB, MySQL, Oracle, and PostgreSQL DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs).

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.

Failover is automatically handled by Amazon RDS so that you can resume database operations as quickly as possible without administrative intervention. 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. Multi-AZ means the URL is the same, the failover is automated, and the CNAME will automatically be updated to point to the standby database.

Incorrect options:

The URL to access the database will change to the standby DB - As discussed above, URL remains the same.

An email will be sent to the System Administrator asking for manual intervention - This option is incorrect and it has been added as a distractor.

The application will be down until the primary database has recovered itself - This option is incorrect and it has been added as a distractor.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

https://aws.amazon.com/rds/faqs/

질문 11: 정답

An application with global users across AWS Regions had suffered an issue when the Elastic Load Balancer (ELB) in a Region malfunctioned thereby taking down the traffic with it. The manual intervention cost the company significant time and resulted in major revenue loss.

What should a solutions architect recommend to reduce internet latency and add automatic failover across AWS Regions?

설명 Correct option:

Set up AWS Global Accelerator and add endpoints to cater to users in different geographic locations

As your application architecture grows, so does the complexity, with longer user-facing IP lists and more nuanced traffic routing logic. AWS Global Accelerator solves this by providing you with two static IPs that are anycast from our globally distributed edge locations, giving you a single entry point to your application, regardless of how many AWS Regions it's deployed in. This allows you to add or remove origins, Availability Zones or Regions without reducing your application availability. Your traffic routing is managed manually, or in console with endpoint traffic dials and weights. If your application endpoint has a failure or availability issue, AWS Global Accelerator will automatically redirect your new connections to a healthy endpoint within seconds.

By using AWS Global Accelerator, you can:

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. The IP addresses are anycast from AWS edge locations so they provide onboarding to the AWS global network close to your users.

Easily move endpoints between Availability Zones or AWS Regions without needing to update your DNS configuration or change client-facing applications.

Dial traffic up or down for a specific AWS Region by configuring a traffic dial percentage for your endpoint groups. This is especially useful for testing performance and releasing updates.

Control the proportion of traffic directed to each endpoint within an endpoint group by assigning weights across the endpoints.

AWS Global Accelerator for Multi-Region applications: via - https://aws.amazon.com/global-accelerator/

Incorrect options:

Set up AWS Direct Connect as the backbone for each of the AWS Regions where the application is deployed - AWS Direct Connect can reduce latency to great extent. Direct Connect is used to connect on-premises systems to AWS Cloud for extremely low latency use cases. It cannot be used to serve users directly.

Create S3 buckets in different AWS Regions and configure CloudFront to pick the nearest edge location to the user - If most of the content is static, we can configure CloudFront to improve performance. In the current scenario, the architecture has ELBs, EC2 instances too that need to be covered in the automatic failover plan.

Set up an Amazon Route 53 geoproximity routing policy to route traffic* - Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. Unlike Global Accelerator, managing and routing to different instances, ELBs and other AWS resources will become an operational overhead as the resource count reaches into the hundreds. With inbuilt features like Static anycast IP addresses, fault tolerance using network zones, Global performance-based routing, TCP Termination at the Edge - Global Accelerator is the right choice for multi-region, low latency use cases.

References:

https://aws.amazon.com/global-accelerator/features/

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geoproximity

질문 12: 오답

A junior developer is learning to build websites using HTML, CSS, and JavaScript. He has created a static website and then deployed it on Amazon S3. Now he can't seem to figure out the endpoint for his super cool website.

As a solutions architect, can you help him figure out the allowed formats for the Amazon S3 website endpoints? (Select two)

설명 Correct options:

http://bucket-name.s3-website.Region.amazonaws.com

http://bucket-name.s3-website-Region.amazonaws.com

To host a static website on Amazon S3, you configure an Amazon S3 bucket for website hosting and then upload your website content to the bucket. When you configure a bucket as a static website, you enable static website hosting, set permissions, and add an index document. Depending on your website requirements, you can also configure other options, including redirects, web traffic logging, and custom error documents.

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket.

Depending on your Region, your Amazon S3 website endpoints follow one of these two formats.

s3-website dash (-) Region - http://bucket-name.s3-website.Region.amazonaws.com

s3-website dot (.) Region - http://bucket-name.s3-website-Region.amazonaws.com

These URLs return the default index document that you configure for the website.

Incorrect options:

http://s3-website-Region.bucket-name.amazonaws.com

http://s3-website.Region.bucket-name.amazonaws.com

http://bucket-name.Region.s3-website.amazonaws.com

These three options do not meet the specifications for the Amazon S3 website endpoints format, so these are incorrect.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteEndpoints.html

질문 14: 정답

A leading video streaming provider is migrating to AWS Cloud infrastructure for delivering its content to users across the world. The company wants to make sure that the solution supports at least a million requests per second for its EC2 server farm.

As a solutions architect, which type of Elastic Load Balancer would you recommend as part of the solution stack?

설명 Correct option:

Network Load Balancer

Network Load Balancer is best suited for use-cases involving low latency and high throughput workloads that involve scaling to millions of requests per second. Network Load Balancer operates at the connection level (Layer 4), routing connections to targets - Amazon EC2 instances, microservices, and containers – within Amazon Virtual Private Cloud (Amazon VPC) based on IP protocol data.

Incorrect options:

Application Load Balancer - Application Load Balancer operates at the request level (layer 7), routing traffic to targets – EC2 instances, containers, IP addresses, and Lambda functions based on the content of the request. Ideal for advanced load balancing of HTTP and HTTPS traffic, Application Load Balancer provides advanced request routing targeted at delivery of modern application architectures, including microservices and container-based applications. Application Load Balancer is not a good fit for the low latency and high throughput scenario mentioned in the given use-case.

Classic Load Balancer - Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network. Classic Load Balancer is not a good fit for the low latency and high throughput scenario mentioned in the given use-case.

Infrastructure Load Balancer - There is no such thing as Infrastructure Load Balancer and this option just acts as a distractor.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

질문 15: 정답

An IT company has built a custom data warehousing solution for a retail organization by using Amazon Redshift. As part of the cost optimizations, the company wants to move any historical data (any data older than a year) into S3, as the daily analytical reports consume data for just the last one year. However the analysts want to retain the ability to cross-reference this historical data along with the daily reports.

The company wants to develop a solution with the LEAST amount of effort and MINIMUM cost. As a solutions architect, which option would you recommend to facilitate this use-case?

설명 Correct option:

Use Redshift Spectrum to create Redshift cluster tables pointing to the underlying historical data in S3. The analytics team can then query this historical data to cross-reference with the daily reports from Redshift

Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis.

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables.

Amazon Redshift Spectrum resides on dedicated Amazon Redshift servers that are independent of your cluster. Redshift Spectrum pushes many compute-intensive tasks, such as predicate filtering and aggregation, down to the Redshift Spectrum layer. Thus, Redshift Spectrum queries use much less of your cluster's processing capacity than other queries.

Redshift Spectrum Overview via - https://aws.amazon.com/blogs/big-data/amazon-redshift-spectrum-extends-data-warehousing-out-to-exabytes-no-loading-required/

Incorrect options:

Setup access to the historical data via Athena. The analytics team can run historical data queries on Athena and continue the daily reporting on Redshift. In case the reports need to be cross-referenced, the analytics team need to export these in flat files and then do further analysis Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to set up or manage, and customers pay only for the queries they run. You can use Athena to process logs, perform ad-hoc analysis, and run interactive queries. Providing access to historical data via Athena would mean that historical data reconciliation would become difficult as the daily report would still be produced via Redshift. Such a setup is cumbersome to maintain on a day to day basis. Hence the option to use Athena is ruled out.

Use the Redshift COPY command to load the S3 based historical data into Redshift. Once the ad-hoc queries are run for the historic data, it can be removed from Redshift

Use Glue ETL job to load the S3 based historical data into Redshift. Once the ad-hoc queries are run for the historic data, it can be removed from Redshift

Loading historical data into Redshift via COPY command or Glue ETL job would cost heavy for a one-time ad-hoc process. The same result can be achieved more cost-efficiently by using Redshift Spectrum. Therefore both these options to load historical data into Redshift are also incorrect for the given use-case.

References:

https://docs.aws.amazon.com/redshift/latest/dg/c-using-spectrum.html#c-spectrum-overview
https://aws.amazon.com/blogs/big-data/

amazon-redshift-spectrum-extends-data-warehousing-out-to-exabytes-no-loading-required/

질문 16: 정답

A retail company maintains a Direct Connect connection to AWS and has recently migrated its data warehouse to AWS. The data analysts at the company query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 60 MB and the query responses returned by the data warehouse are not cached in the visualization tool. Each webpage returned by the visualization tool is approximately 600 KB.

Which of the following options offers the LOWEST data transfer egress cost for the company?

설명 Correct option:

Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over a Direct Connect connection at a location in the same region

AWS Direct Connect is a networking service that provides an alternative to using the internet to connect to AWS. Using AWS Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your on-premises data center and AWS.

For the given use case, the main pricing parameter while using the Direct Connect connection is the Data Transfer Out (DTO) from AWS to the on-premises data center. DTO refers to the cumulative network traffic that is sent through AWS Direct Connect to destinations outside of AWS. This is charged per gigabyte (GB), and unlike capacity measurements, DTO refers to the amount of data transferred, not the speed.

via - https://aws.amazon.com/directconnect/pricing/

Each query response is 60MB in size and each webpage for the visualization tool is 600KB in size. If you deploy the visualization tool in the same AWS region as the data warehouse, then you only need to pay for the 600KB of DTO charges for the webpage. Therefore this option is correct.

However, if you deploy the visualization tool on-premises, then you need to pay for the 60 MB of DTO charges for the query response from the data warehouse to the visualization tool.

Incorrect options:

Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over the internet at a location in the same region

Deploy the visualization tool on-premises. Query the data warehouse over the internet at a location in the same AWS region

Data transfer pricing over Direct Connect is lower than data transfer pricing over the internet, so both of these options are incorrect.

Deploy the visualization tool on-premises. Query the data warehouse directly over a Direct Connect connection at a location in the same AWS region - As mentioned in the explanation above, if you deploy the visualization tool on-premises, then you need to pay for the 60 MB of DTO charges for the query response from the data warehouse to the visualization tool. So this option is incorrect.

References:

https://aws.amazon.com/directconnect/pricing/

https://aws.amazon.com/getting-started/hands-on/connect-data-center-to-aws/services-costs/

https://aws.amazon.com/directconnect/faqs/

질문 17: 오답

The engineering team at an e-commerce company uses a Lambda function to write the order data into a single DB instance Aurora cluster. The team has noticed that many order- writes to its Aurora cluster are

getting missed during peak load times. The diagnostics data has revealed that the DB is experiencing high CPU and memory consumption during traffic spikes. The team also wants to enhance the availability of the Aurora DB.

Which of the following steps would you combine to address the given scenario? (Select two)

설명 Correct options:

Handle all read operations for your application by connecting to the reader endpoint of the Aurora cluster so that Aurora can spread the load for read-only connections across the Aurora replica

When you create a second, third, and so on DB instance in an Aurora-provisioned DB cluster, Aurora automatically sets up replication from the writer DB instance to all the other DB instances. These other DB instances are read-only and are known as Aurora Replicas.

Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer.

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

Create a replica Aurora instance in another Availability Zone to improve the availability as the replica can serve as a failover target

If the primary instance in a DB cluster using single-master replication fails, Aurora automatically fails over to a new primary instance in one of two ways:

By promoting an existing Aurora Replica to the new primary instance By creating a new primary instance

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html

Incorrect options:

Create a standby Aurora instance in another Availability Zone to improve the availability as the standby can serve as a failover target - There are no standby instances in Aurora. Aurora performs an automatic failover to a read replica when a problem is detected. So this option is incorrect.

Read replicas, Multi-AZ deployments, and multi-region deployments: via - https://aws.amazon.com/rds/features/read-replicas/

Increase the concurrency of the Lambda function so that the order-writes do not get missed during traffic spikes - Increasing the concurrency of the Lambda function would not resolve the issue since the bottleneck is at the database layer, as exhibited by the high CPU and memory consumption for the Aurora instance. This option has been added as a distractor.

Use EC2 instances behind an Application Load Balancer to write the order data into the Aurora cluster - Using EC2 instances behind an Application Load Balancer would not resolve the issue since the bottleneck is at the database layer, as exhibited by the high CPU and memory consumption for the Aurora instance. This option has been added as a distractor.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html

https://aws.amazon.com/rds/features/read-replicas/

질문 18: 정답

A medium-sized business has a taxi dispatch application deployed on an EC2 instance. Because of an unknown bug, the application causes the instance to freeze regularly. Then, the instance has to be manually restarted via the AWS management console.

Which of the following is the MOST cost-optimal and resource-efficient way to implement an automated solution until a permanent fix is delivered by the development team?

설명 Correct option:

Setup a CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, an EC2 Reboot CloudWatch Alarm Action can be used to reboot the instance

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.

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance. The reboot alarm action is recommended for Instance Health Check failures (as opposed to the recover alarm action, which is suited for System Health Check failures).

Incorrect options:

Setup a CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, CloudWatch Alarm can publish to an SNS event which can then trigger a lambda function. The lambda function can use AWS EC2 API to reboot the instance

Use EventBridge events to trigger a Lambda function to check the instance status every 5 minutes. In the case of Instance Health Check failure, the lambda function can use AWS EC2 API to reboot the instance

Use EventBridge events to trigger a Lambda function to reboot the instance status every 5 minutes

Using EventBridge event or CloudWatch alarm to trigger a lambda function, directly or indirectly, is wasteful of resources. You should just use the EC2 Reboot CloudWatch Alarm Action to reboot the instance. So all the options that trigger the lambda function are incorrect.

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html

질문 19: 정답

A silicon valley based startup helps its users legally sign highly confidential contracts. To meet the compliance guidelines, the startup must ensure that the signed contracts are encrypted using the AES-256 algorithm via an encryption key that is generated internally. The startup is now migrating to AWS Cloud and would like the data to be encrypted on AWS. The startup wants to continue using their existing encryption key generation mechanism.

What do you recommend?

설명 Correct option:

SSE-C - With 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. With SSE-C, the startup can still provide the encryption key but let AWS do the encryption. Therefore, this is the correct option.

Incorrect options:

SSE-KMS - 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. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created. But, you never get to know the actual key here.

SSE-S3 - When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. However, this option does not provide the ability to audit trail the usage of the encryption keys.

Client-Side Encryption - Client-side encryption is the act of encrypting data before sending it to Amazon S3. To enable client-side encryption, you have the following options: Use a customer master key (CMK) stored in AWS Key Management Service (AWS KMS), Use a master key you store within your application. Since the customer wants to use AWS provided facility, this is not an option.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

질문 21: 정답

A global media company uses a fleet of EC2 instances (behind an Application Load Balancer) to power its video streaming application. To improve the performance of the application, the engineering team has also created a CloudFront distribution with the Application Load Balancer as the custom origin. The security team at the company has noticed a spike in the number and types of SQL injection and cross-site scripting attack vectors on the application.

As a solutions architect, which of the following solutions would you recommend as the MOST effective in countering these malicious attacks?

설명 Correct option:

Use Web Application Firewall (WAF) with CloudFront distribution

AWS WAF is 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 WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

How WAF Works: via - https://aws.amazon.com/waf/

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distribution, Amazon API Gateway API, or Application Load Balancer responds to.

When you create a web ACL, you can specify one or more CloudFront distributions that you want AWS WAF to inspect. AWS WAF starts to allow, block, or count web requests for those distributions based on the conditions that you identify in the web ACL. Therefore, combining WAF with CloudFront can prevent SQL injection and cross-site scripting attacks. So this is the correct option.

Incorrect options:

Use Route 53 with CloudFront distribution - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. You cannot use Route 53 to prevent SQL injection and cross-site scripting attacks. So this option is incorrect.

Use Security Hub with CloudFront distribution - AWS Security Hub gives you a comprehensive view of your high-priority security alerts and security posture across your AWS accounts. With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, as well as from AWS Partner solutions. You cannot use Security Hub to prevent SQL injection and cross-site scripting attacks. So this option is incorrect.

Use AWS Firewall Manager with CloudFront distribution - AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization. You cannot use Firewall Manager to prevent SQL injection and cross-site scripting attacks. So this option is incorrect.

References:

https://aws.amazon.com/waf/features/

https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html

질문 22: 오답

A leading media company wants to do an accelerated online migration of hundreds of terabytes of files from their on-premises data center to Amazon S3 and then establish a mechanism to access the migrated data for ongoing updates from the on-premises applications.

As a solutions architect, which of the following would you select as the MOST performant solution for the given use-case?

설명 Correct options:

Use AWS DataSync to migrate existing data to Amazon S3 and then use File Gateway to retain access to the migrated data for ongoing updates from the on-premises applications

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data to and from AWS storage services over the internet or AWS Direct Connect.

AWS DataSync fully automates and accelerates moving large active datasets to AWS, up to 10 times faster than command-line tools. It is natively integrated with Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon CloudWatch, and AWS CloudTrail, which provides seamless and secure access to your storage services, as well as detailed monitoring of the transfer. DataSync uses a purpose-built network protocol and scale-out architecture to transfer data. A single DataSync agent is capable of saturating a 10 Gbps network link.

DataSync fully automates the data transfer. It comes with retry and network resiliency mechanisms, network optimizations, built-in task scheduling, monitoring via the DataSync API and Console, and CloudWatch metrics, events, and logs that provide granular visibility into the transfer process. DataSync performs data integrity verification both during the transfer and at the end of the transfer.

How DataSync Works: via - https://aws.amazon.com/datasync/

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. The service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

The combination of DataSync and File Gateway is the correct solution. AWS DataSync enables you to automate and accelerate online data transfers to AWS storage services. File Gateway then provides your on-premises applications with low latency access to the migrated data.

Incorrect options:

Use AWS DataSync to migrate existing data to Amazon S3 as well as access the S3 data for ongoing updates - AWS DataSync is used to easily transfer data to and from AWS with up to 10x faster speeds. It is used to transfer data and cannot be used to facilitate ongoing updates to the migrated files from the on-premises applications.

Use File Gateway configuration of AWS Storage Gateway to migrate data to Amazon S3 and then use S3 Transfer Acceleration for ongoing updates from the on-premises applications - File Gateway can be used to move on-premises data to AWS Cloud, but it not an optimal solution for high volumes. Migration services such as DataSync are best suited for this purpose. S3 Transfer Acceleration cannot facilitate ongoing updates to the migrated files from the on-premises applications.

Use S3 Transfer Acceleration to migrate existing data to Amazon S3 and then use DataSync for ongoing updates from the on-premises applications - If your application is already integrated with the Amazon S3 API, and you want higher throughput for transferring large files to S3, S3 Transfer Acceleration can be used.

However DataSync cannot be used to facilitate ongoing updates to the migrated files from the on-premises applications.

Reference:

https://aws.amazon.com/datasync/features/

질문 23: 정답

Your firm has implemented a multi-tiered networking structure within the VPC - with two public and two private subnets. The public subnets are used to deploy the Application Load Balancers, while the two private subnets are used to deploy the application on Amazon EC2 instances. The development team wants the EC2 instances to have access to the internet. The solution has to be fully managed by AWS and needs to work over IPv4.

What will you recommend?

설명 Correct option:

NAT Gateways deployed in your public subnet - 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. A NAT gateway has the following characteristics and limitations:

A NAT gateway supports 5 Gbps of bandwidth and automatically scales up to 45 Gbps. You can associate exactly one Elastic IP address with a NAT gateway. A NAT gateway supports the following protocols: TCP, UDP, and ICMP. You cannot associate a security group with a NAT gateway. You can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located. A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. Therefore you must use a NAT Gateway in your public subnet in order to provide internet access to your instances in your private subnets. You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply.

Comparison of NAT instances and NAT gateways: via - https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Incorrect options:

NAT Instances deployed in your public subnet - You can use a network address translation (NAT) instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the Internet. Amazon provides Amazon Linux AMIs that are configured to run as NAT instances. These AMIs include the string amzn-ami-vpc-nat in their names, so you can search for them in the Amazon EC2 console. NAT Instances would work but won't scale and you would have to manage them (as they're nothing but EC2 instances).

Internet Gateways deployed in your private subnet - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic. Internet Gateways must be deployed in a public subnet, hence not an option here.

Egress-Only Internet Gateways deployed in your private subnet - 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. Egress-Only Internet Gateways are for IPv6, not IPv4. Therefore, this option is incorrect.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html

질문 24: 정답

Your company is evolving towards a microservice approach for their website. The company plans to expose the website from the same load balancer, linked to different target groups with different URLs, that are similar to these - checkout.mycorp.com, www.mycorp.com, mycorp.com/profile, and mycorp.com/search.

As a Solutions Architect, which Load Balancer type do you recommend to achieve this routing feature with MINIMUM configuration and development effort?

설명 Correct option:

Create an Application Load Balancer

Application Load Balancer can automatically distribute 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.

If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request.

Here are the different types -

Host-based Routing: You can route a client request based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer. You can use host conditions to define rules that route requests based on the hostname in the host header (also known as host-based routing). This enables you to support multiple domains using a single load balancer. Example hostnames: example.com test.example.com *.example.com The rule *.example.com matches test.example.com but doesn't match example.com.

Path-based Routing: You can route a client request based on the URL path of the HTTP header. You can use path conditions to define rules that route requests based on the URL in the request (also known as path-based routing). Example path patterns: /img/* /img//pics The path pattern is used to route requests but does not alter them. For example, if a rule has a path pattern of /img/, the rule would forward a request for /img/picture.jpg to the specified target group as a request for /img/picture.jpg. The path pattern is applied only to the path of the URL, not to its query parameters.

HTTP header-based routing: You can route a client request based on the value of any standard or custom HTTP header.

HTTP method-based routing: You can route a client request based on any standard or custom HTTP method.

Query string parameter-based routing: You can route a client request based on query string or query parameters.

Source IP address CIDR-based routing: You can route a client request based on source IP address CIDR from where the request originates.

Path based routing and host based routing are only available for the Application Load Balancer (ALB). Therefore this is the correct option for the given use-case.

Incorrect options:

Create an NGINX based load balancer on an EC2 instance to have advanced routing capabilities - Although it is technically possible to set up NGINX based load balancer, however, this option involves a lot of configuration effort, so this option is ruled out for the given use-case. So, deploying an NGINX load balancer on EC2 would work but would suffer management and scaling issues.

Create a Network Load Balancer - Network Load Balancer is best suited for use-cases involving low latency and high throughput workloads that involve scaling to millions of requests per second. Network Load Balancer operates at the connection level (Layer 4), routing connections to targets - Amazon EC2 instances, microservices, and containers – within Amazon Virtual Private Cloud (Amazon VPC) based on IP protocol data.

Create a Classic Load Balancer - Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

As mentioned in the description above, these two options are incorrect for the given use-case.

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

https://aws.amazon.com/blogs/aws/new-host-based-routing-support-for-aws-application-load-balancers/

질문 25: 오답

A mobile chat application uses DynamoDB as its database service to provide low latency chat updates. A new developer has joined the team and is reviewing the configuration settings for DynamoDB which have been tweaked for certain technical requirements. CloudTrail service has been enabled on all the resources used for the project. Yet, DynamoDB encryption details are nowhere to be found.

Which of the following options can explain the root cause for the given issue?

설명 Correct option:

By default, all DynamoDB tables are encrypted under an AWS owned customer master key (CMK), which do not write to CloudTrail logs - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. Although AWS owned CMKs are not in your AWS account, an AWS service can use its AWS owned CMKs to protect the resources in your account.

You do not need to create or manage the AWS owned CMKs. However, you cannot view, use, track, or audit them. You are not charged a monthly fee or usage fee for AWS owned CMKs and they do not count against the AWS KMS quotas for your account.

The key rotation strategy for an AWS owned CMK is determined by the AWS service that creates and manages the CMK.

All DynamoDB tables are encrypted. There is no option to enable or disable encryption for new or existing tables. By default, all tables are encrypted under an AWS owned customer master key (CMK) in the DynamoDB service account. However, you can select an option to encrypt some or all of your tables under a customer-managed CMK or the AWS managed CMK for DynamoDB in your account.

Incorrect options:

By default, all DynamoDB tables are encrypted under AWS managed CMKs, which do not write to CloudTrail logs

By default, all DynamoDB tables are encrypted under Customer managed CMKs, which do not write to CloudTrail logs

By default, all DynamoDB tables are encrypted using Data keys, which do not write to CloudTrail logs

These three options contradict the explanation provided above, so these options are incorrect.

References:

https://docs.aws.amazon.com/kms/latest/developerguide/services-dynamodb.html

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

질문 28: 정답

A media company wants to get out of the business of owning and maintaining its own IT infrastructure. As part of this digital transformation, the media company wants to archive about 5PB of data in its on-premises data center to durable long term storage.

As a solutions architect, what is your recommendation to migrate this data in the MOST cost-optimal way?

설명 Correct option:

Transfer the on-premises data into multiple Snowball Edge Storage Optimized devices. Copy the Snowball Edge data into Amazon S3 and create a lifecycle policy to transition the data into AWS Glacier

Snowball Edge Storage Optimized is the optimal choice if you need to securely and quickly transfer dozens of terabytes to petabytes of data to AWS. It provides up to 80 TB of usable HDD storage, 40 vCPUs, 1 TB of SATA SSD storage, and up to 40 Gb network connectivity to address large scale data transfer and pre-processing use cases. The data stored on the Snowball Edge device can be copied into the S3 bucket and later transitioned into AWS Glacier via a lifecycle policy. You can't directly copy data from Snowball Edge devices into AWS Glacier.

Incorrect options:

Transfer the on-premises data into multiple Snowball Edge Storage Optimized devices. Copy the Snowball Edge data into AWS Glacier - As mentioned earlier, you can't directly copy data from Snowball Edge devices into AWS Glacier. Hence, this option is incorrect.

Setup AWS direct connect between the on-premises data center and AWS Cloud. Use this connection to transfer the data into AWS Glacier - AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. Direct Connect involves significant monetary investment and takes more than a month to set up, therefore it's not the correct fit for this use-case where just a one-time data transfer has to be done.

Setup Site-to-Site VPN connection between the on-premises data center and AWS Cloud. Use this connection to transfer the data into AWS Glacier - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). VPN Connections are a good solution if you have an immediate need, and have low to modest bandwidth requirements. Because of the high data volume for the given use-case, Site-to-Site VPN is not the correct choice.

Reference:

https://aws.amazon.com/snowball/

질문 29: 정답

A retail company wants to establish encrypted network connectivity between its on-premises data center and AWS Cloud. The company wants to get the solution up and running in the fastest possible time and it should also support encryption in transit.

As a solutions architect, which of the following solutions would you suggest to the company?

설명 Correct options:

Use Site-to-Site VPN to establish encrypted network connectivity between the on-premises data center and AWS Cloud

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your on-premises network and Amazon VPC over the Internet. IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet in a data stream.

Incorrect options:

Use AWS Direct Connect to establish encrypted network connectivity between the on-premises data center and AWS Cloud - AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. AWS Direct Connect does not encrypt your traffic that is in transit. To encrypt the data in transit that traverses AWS Direct Connect, you must use the transit encryption options for that service. As AWS Direct Connect does not support

encrypted network connectivity between an on-premises data center and AWS Cloud, therefore this option is incorrect.

Use AWS Data Sync to establish encrypted network connectivity between the on-premises data center and AWS Cloud - AWS DataSync makes it simple and fast to move large amounts of data online between on-premises storage and AWS. DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling, and monitoring transfers, validating data, and optimizing network utilization. As AWS Data Sync cannot be used to establish network connectivity between an on-premises data center and AWS Cloud, therefore this option is incorrect.

Use AWS Secrets Manager to establish encrypted network connectivity between the on-premises data center and AWS Cloud - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. As AWS Secrets Manager cannot be used to establish network connectivity between an on-premises data center and AWS Cloud, therefore this option is incorrect.

References:

https://docs.aws.amazon.com/vpn/latest/s2svpn/internetwork-traffic-privacy.html

https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html

질문 32: 정답

The engineering team at a retail company manages 3 Amazon EC2 instances that make read-heavy database requests to the Amazon RDS for the PostgreSQL DB instance. As an AWS Certified Solutions Architect Associate, you have been tasked to make the database instance resilient from a disaster recovery perspective.

Which of the following features will help you in disaster recovery of the database? (Select two)

설명 Correct option:

Use cross-Region Read Replicas

In addition to using Read Replicas to reduce the load on your source DB instance, you can also use Read Replicas to implement a DR solution for your production DB environment. If the source DB instance fails, you can promote your Read Replica to a standalone source server. Read Replicas can also be created in a different Region than the source database. Using a cross-Region Read Replica can help ensure that you get back up and running if you experience a regional availability issue.

Enable the automated backup feature of Amazon RDS in a multi-AZ deployment that creates backups across multiple Regions

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 MariaDB, MySQL, Oracle, and PostgreSQL DB instances use Amazon's failover technology.

The automated backup feature of Amazon RDS enables point-in-time recovery for your database instance. Amazon RDS will back up your database and transaction logs and store both for a user-specified retention

period. If it's a Multi-AZ configuration, backups occur on standby to reduce the I/O impact on the primary. Amazon RDS supports Cross-Region Automated Backups. Manual snapshots and Read Replicas are also supported across multiple Regions.

Incorrect options:

Enable the automated backup feature of Amazon RDS in a multi-AZ deployment that creates backups in a single AWS Region - This is an incorrect statement. Automated backups can be created across AWS Regions.

Use RDS Provisioned IOPS (SSD) Storage in place of General Purpose (SSD) Storage - Amazon RDS Provisioned IOPS Storage is an SSD-backed storage option designed to deliver fast, predictable, and consistent I/O performance. This storage type enhances the performance of the RDS database, but this isn't a disaster recovery option.

Use the database cloning feature of the RDS DB cluster - This option has been added as a distractor. Database cloning is only available for Aurora and not for RDS.

References:

https://aws.amazon.com/rds/features/

https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/

https://aws.amazon.com/about-aws/whats-new/2021/07/amazon-rds-cross-region-automated-backups-regional-expansion/

질문 33: 오답

You have built an application that is deployed with an Elastic Load Balancer and an Auto Scaling Group. As a Solutions Architect, you have configured aggressive CloudWatch alarms, making your Auto Scaling Group (ASG) scale in and out very quickly, renewing your fleet of Amazon EC2 instances on a daily basis. A production bug appeared two days ago, but the team is unable to SSH into the instance to debug the issue, because the instance has already been terminated by the ASG. The log files are saved on the EC2 instance.

How will you resolve the issue and make sure it doesn't happen again?

설명 Correct option:

Install a CloudWatch Logs agents on the EC2 instances to send logs to CloudWatch

You can use the CloudWatch Logs agent installer on an existing EC2 instance to install and configure the CloudWatch Logs agent. After installation is complete, logs automatically flow from the instance to the log stream you create while installing the agent. The agent confirms that it has started and it stays running until you disable it.

Here, the natural and by far the easiest solution would be to use the CloudWatch Logs agents on the EC2 instances to automatically send log files into CloudWatch, so we can analyze them in the future easily should any problem arise.

To control whether an Auto Scaling group can terminate a particular instance when scaling in, use instance scale-in protection. You can enable the instance scale-in protection setting on an Auto Scaling group or on

an individual Auto Scaling instance. When the Auto Scaling group launches an instance, it inherits the instance scale-in protection setting of the Auto Scaling group. You can change the instance scale-in protection setting for an Auto Scaling group or an Auto Scaling instance at any time.

Incorrect options:

Disable the Termination from the ASG any time a user reports an issue - Disabling the Termination from the ASG would prevent our ASG from being Elastic and impact our costs. Therefore this option is incorrect.

Make a snapshot of the EC2 instance just before it gets terminated - Making a snapshot of the EC2 instance before it gets terminated could work but it's tedious, not elastic and very expensive, since our interest is just the log files. Therefore this option is not the best fit for the given use-case.

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.

Use AWS Lambda to regularly SSH into the EC2 instances and copy the log files to S3 - AWS Lambda lets you run code without provisioning or managing servers. It cannot be used for production-grade serverless log analytics. Using AWS Lambda would be extremely hard to use for this task. Therefore this option is not the best fit for the given use-case.

Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html

질문 36: 정답

A big data analytics company is using Kinesis Data Streams (KDS) to process IoT data from the field devices of an agricultural sciences company. Multiple consumer applications are using the incoming data streams and the engineers have noticed a performance lag for the data delivery speed between producers and consumers of the data streams.

As a solutions architect, which of the following would you recommend for improving the performance for the given use-case?

설명 Correct option:

Use Enhanced Fanout feature of Kinesis Data Streams

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

By default, the 2MB/second/shard output is shared between all of the applications consuming data from the stream. You should use enhanced fan-out if you have multiple consumers retrieving data from a stream in parallel. With enhanced fan-out developers can register stream consumers to use enhanced fan-out and receive their own 2MB/second pipe of read throughput per shard, and this throughput automatically scales with the number of shards in a stream.

Kinesis Data Streams Fanout via - https://aws.amazon.com/blogs/aws/kds-enhanced-fanout/

Incorrect options:

Swap out Kinesis Data Streams with Kinesis Data Firehose - Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data lakes, data stores, and analytics tools. 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, transform, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security. Kinesis Data Firehose can only write to S3, Redshift, Elasticsearch or Splunk. You can't have applications consuming data streams from Kinesis Data Firehose, that's the job of Kinesis Data Streams. Therefore this option is not correct.

Swap out Kinesis Data Streams with SQS Standard queues

Swap out Kinesis Data Streams with SQS FIFO queues

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 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. As multiple applications are consuming the same stream concurrently, both SQS Standard and SQS FIFO are not the right fit for the given use-case.

Exam Alert:

Please understand the differences between the capabilities of Kinesis Data Streams vs SQS, as you may be asked scenario-based questions on this topic in the exam.

via - https://aws.amazon.com/kinesis/data-streams/faqs/

References:

https://aws.amazon.com/blogs/aws/kds-enhanced-fanout/

https://aws.amazon.com/kinesis/data-streams/faqs/

질문 37: 정답

A financial services company runs its flagship web application on AWS. The application serves thousands of users during peak hours. The company needs a scalable near-real-time solution to share hundreds of thousands of financial transactions with multiple internal applications. The solution should also remove sensitive details from the transactions before storing the cleansed transactions in a document database for low-latency retrieval.

As an AWS Certified Solutions Architect Associate, which of the following would you recommend?

설명 Correct option:

Feed the streaming transactions into Amazon Kinesis Data Streams. Leverage Amazon Lambda integration to remove sensitive data from every transaction and then store the cleansed transactions in DynamoDB. The internal applications can consume the raw transactions off the Kinesis Data Stream

You can use Kinesis Data Streams to build custom applications that process or analyze streaming data for specialized needs. Kinesis Data Streams manages the infrastructure, storage, networking, and configuration needed to stream your data at the level of your data throughput. You don't have to worry about provisioning, deployment, or ongoing maintenance of hardware, software, or other services for your data streams.

How Kinesis Data Streams Work: via - https://aws.amazon.com/kinesis/data-streams/

Kinesis Data Streams Key Concepts: via - https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html

For the given use case, you can stream the raw financial transactions into Kinesis Data Streams, which in turn, are processed by the Lambda function that is set up as one of the consumers of the data stream. The Lambda would remove sensitive data from every transaction and then store the cleansed transactions in DynamoDB. The internal applications can be configured as the other consumers of the data stream and ingest the raw transactions

Incorrect options:

Batch process the raw transactions data into Amazon S3 flat files. Use S3 events to trigger an Amazon Lambda function to remove sensitive data from the raw transactions in the flat file and then store the cleansed transactions in DynamoDB. Leverage DynamoDB Streams to share the transactions data with the internal applications - The use case requires a near-real-time solution for cleansing, processing and storing the transactions, so using a batch process would be incorrect.

Feed the streaming transactions into Amazon Kinesis Data Firehose. Leverage Amazon Lambda integration to remove sensitive data from every transaction and then store the cleansed transactions in DynamoDB. The internal applications can consume the raw transactions off the Kinesis Data Firehose - Amazon Kinesis Data Firehose is an extract, transform, and load (ETL) service that reliably captures, transforms, and delivers streaming data to data lakes, data stores, and analytics services.

via - https://aws.amazon.com/kinesis/data-firehose/

You cannot set up multiple consumers for Kinesis Data Firehose delivery streams as it can dump data in a single data repository at a time, so this option is incorrect.

Persist the raw transactions into Amazon DynamoDB. Configure a rule in DynamoDB to update the transaction by removing sensitive data whenever any new raw transaction is written. Leverage DynamoDB Streams to share the transactions data with the internal applications - There is no such rule within DynamoDB that can auto-update every time a new item is written in a DynamoDB table. You would need to use a DynamoDB trigger to invoke an external service like a Lambda function on every new write, which can then cleanse and update the item. In addition, this process introduces inefficiency in the workflow as the same item is written and then updated for cleansing purposes. Therefore this option is incorrect.

References:

https://aws.amazon.com/kinesis/data-streams/

https://aws.amazon.com/kinesis/data-firehose/

https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html

질문 38: 정답

A cyber security company is running a mission critical application using a single Spread placement group of EC2 instances. The company needs 15 Amazon EC2 instances for optimal performance.

How many Availability Zones (AZs) will the company need to deploy these EC2 instances per the given use-case?

설명 Correct option:

3

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, you can create a placement group using one of the following placement strategies:

Cluster placement group

Partition placement group

Spread placement group.

A Spread placement group is a group of instances that are each placed on distinct racks, with each rack having its own network and power source.

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.

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. Therefore, to deploy 15 EC2 instances in a single Spread placement group, the company needs to use 3 AZs.

Spread placement group overview: via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Incorrect options:

7

14

15

These three options contradict the details provided in the explanation above, so these options are incorrect.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

질문 40: 오답

A health-care company manages its web application on Amazon EC2 instances running behind Auto Scaling group (ASG). The company provides ambulances for critical patients and needs the application to be reliable. The workload of the company can be managed on 2 EC2 instances and can peak up to 6 instances when traffic increases.

As a Solutions Architect, which of the following configurations would you select as the best fit for these requirements?

설명 Correct option:

The ASG should be configured with the minimum capacity set to 4, with 2 instances each in two different Availability Zones. The maximum capacity of the ASG should be set to 6 - You configure the size of your Auto Scaling group by setting the minimum, maximum, and desired capacity. The minimum and maximum capacity are required to create an Auto Scaling group, while the desired capacity is optional. If you do not define your desired capacity upfront, it defaults to your minimum capacity.

Amazon EC2 Auto Scaling enables you to take advantage of the safety and reliability of geographic redundancy by spanning Auto Scaling groups across multiple Availability Zones within a Region. When one Availability Zone becomes unhealthy or unavailable, Auto Scaling launches new instances in an unaffected Availability Zone. When the unhealthy Availability Zone returns to a healthy state, Auto Scaling automatically redistributes the application instances evenly across all of the designated Availability Zones. Since the application is extremely critical and needs to have a reliable architecture to support it, the EC2 instances should be maintained in at least two Availability Zones (AZs) for uninterrupted service.

Amazon EC2 Auto Scaling attempts to distribute instances evenly between the Availability Zones that are enabled for your Auto Scaling group. This is why the minimum capacity should be 4 instances and not 2. ASG will launch 2 instances each in both the AZs and this redundancy is needed to keep the service available always.

Incorrect options:

The ASG should be configured with the minimum capacity set to 2, with 1 instance each in two different Availability Zones. The maximum capacity of the ASG should be set to 6

The ASG should be configured with the minimum capacity set to 2 and the maximum capacity set to 6 in a single Availability Zone

The explanation above gives the correct rationale for minimum capacity as well as the instance distribution across AZs, so both these options are incorrect.

The ASG should be configured with the minimum capacity set to 4, with 2 instances each in two different AWS Regions. The maximum capacity of the ASG should be set to 6 - An Auto Scaling group can contain EC2 instances in one or more Availability Zones within the same region. However, Auto Scaling groups cannot span multiple Regions.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html

질문 41: 오답

The engineering team at a weather tracking company wants to enhance the performance of its relation database and is looking for a caching solution that supports geospatial data.

As a solutions architect, which of the following solutions will you suggest?

설명 Correct option:

Use Amazon ElastiCache for Redis - Amazon ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. Redis, which stands for Remote Dictionary Server, is a fast, open-source, in-memory key-value data store for use as a database, cache, message broker, and queue. Redis now delivers sub-millisecond response times enabling millions of requests per second for real-time applications in Gaming, Ad-Tech, Financial Services, Healthcare, and IoT. Redis is a popular choice for caching, session management, gaming, leaderboards, real-time analytics, geospatial, ride-hailing, chat/messaging, media streaming, and pub/sub apps.

All Redis data resides in the server's main memory, in contrast to databases such as PostgreSQL, Cassandra, MongoDB and others that store most data on disk or on SSDs. In comparison to traditional disk based databases where most operations require a roundtrip to disk, in-memory data stores such as Redis don't suffer the same penalty. They can therefore support an order of magnitude more operations and faster response times. The result is – blazing fast performance with average read or write operations taking less than a millisecond and support for millions of operations per second.

Redis has purpose-built commands for working with real-time geospatial data at scale. You can perform operations like finding the distance between two elements (for example people or places) and finding all elements within a given distance of a point.

Incorrect options:

Use Amazon ElastiCache for Memcached - Both Redis and MemCached are in-memory, open-source data stores. Memcached, a high-performance distributed memory cache service, is designed for simplicity while Redis offers a rich set of features that make it effective for a wide range of use cases. Memcached does not offer support for geospatial data.

via - https://aws.amazon.com/elasticache/redis-vs-memcached/

Amazon DynamoDB Accelerator (DAX) - Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB. DAX does not support relational databases.

AWS Global Accelerator - AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. This option has been added as a distractor, it has nothing to do with database caching.

Reference:

https://aws.amazon.com/elasticache/redis-vs-memcached/

질문 42: 오답

A financial services company is moving its IT infrastructure to AWS Cloud and wants to enforce adequate data protection mechanisms on Amazon S3 to meet compliance guidelines. The engineering team has hired you as a solutions architect to build a solution for this requirement.

Can you help the team identify the INCORRECT option from the choices below?

설명 Correct option:

S3 can encrypt object metadata by using Server-Side Encryption

Amazon S3 is a simple key-value store designed to store as many objects as you want. You store these objects in one or more buckets, and each object can be up to 5 TB in size.

An object consists of the following:

Key – The name that you assign to an object. You use the object key to retrieve the object.

Version ID – Within a bucket, a key and version ID uniquely identify an object.

Value – The content that you are storing.

Metadata – A set of name-value pairs with which you can store information regarding the object.

Subresources – Amazon S3 uses the subresource mechanism to store object-specific additional information.

Access Control Information – You can control access to the objects you store in Amazon S3.

Metadata, which can be included with the object, is not encrypted while being stored on Amazon S3. Therefore, AWS recommends that customers not place sensitive information in Amazon S3 metadata.

Incorrect options:

S3 can protect data at rest using Server-Side Encryption - This is possible and AWS provides three different ways of doing this - Server-side encryption with Amazon S3-managed keys (SSE-S3), Server-side encryption with customer master keys stored in AWS Key Management Service (SSE-KMS), Server-side encryption with customer-provided keys (SSE-C).

S3 can protect data at rest using Client-Side Encryption - This is a possible scenario too. You can encrypt data on the client-side and upload the encrypted data to Amazon S3. In this case, the client manages the encryption process, the encryption keys, and related tools.

S3 can encrypt data in transit using HTTPS (TLS) - This is also possible and you can use HTTPS (TLS) to help prevent potential attackers from eavesdropping on or manipulating network traffic using person-in-the-middle or similar attacks.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html#server-side

https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf?did=wp_card&trk=wp_card

질문 43: 정답

A company has noticed that its application performance has deteriorated after a new Auto Scaling group was deployed a few days back. Upon investigation, the team found out that the Launch Configuration

selected for the Auto Scaling group is using the incorrect instance type that is not optimized to handle the application workflow.

As a solutions architect, what would you recommend to provide a long term resolution for this issue?

설명 Correct option:

Create a new launch configuration to use the correct instance type. Modify the Auto Scaling group to use this new launch configuration. Delete the old launch configuration as it is no longer needed

A launch configuration is an instance configuration template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances. Include the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping.

It is not possible to modify a launch configuration once it is created. The correct option is to create a new launch configuration to use the correct instance type. Then modify the Auto Scaling group to use this new launch configuration. Lastly to clean-up, just delete the old launch configuration as it is no longer needed.

Incorrect options:

Modify the launch configuration to use the correct instance type and continue to use the existing Auto Scaling group - As mentioned earlier, it is not possible to modify a launch configuration once it is created. Hence, this option is incorrect.

No need to modify the launch configuration. Just modify the Auto Scaling group to use the correct instance type - You cannot use an Auto Scaling group to directly modify the instance type of the underlying instances. Hence, this option is incorrect.

No need to modify the launch configuration. Just modify the Auto Scaling group to use more number of existing instance types. More instances may offset the loss of performance - Using the Auto Scaling group to increase the number of instances to cover up for the performance loss is not recommended as it does not address the root cause of the problem. The Machine Learning workflow requires a certain instance type that is optimized to handle Machine Learning computations. Hence, this option is incorrect.

Reference:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html

질문 45: 오답

A company wants to publish an event into an SQS queue whenever a new object is uploaded on S3.

Which of the following statements are true regarding this functionality?

설명 Correct option:

Only Standard SQS queue is allowed as an Amazon S3 event notification destination, whereas FIFO SQS queue is not allowed

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.

Amazon S3 supports the following destinations where it can publish events:

Amazon Simple Notification Service (Amazon SNS) topic

Amazon Simple Queue Service (Amazon SQS) queue

AWS Lambda

Currently, the Standard SQS queue is only allowed as an Amazon S3 event notification destination, whereas the FIFO SQS queue is not allowed.

Incorrect options:

Both Standard SQS queue and FIFO SQS queue are allowed as an Amazon S3 event notification destination

Neither Standard SQS queue nor FIFO SQS queue is allowed as an Amazon S3 event notification destination

Only FIFO SQS queue is allowed as an Amazon S3 event notification destination, whereas Standard SQS queue is not allowed

These three options contradict the details provided in the explanation above. To summarize, the Standard SQS queue is only allowed as an Amazon S3 event notification destination, whereas the FIFO SQS queue is not allowed. Hence these three options are incorrect.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

질문 46: 오답

A DevOps engineer at an IT company was recently added to the admin group of the company's AWS account. The AdministratorAccess managed policy is attached to this group.

Can you identify the AWS tasks that the DevOps engineer CANNOT perform even though he has full Administrator privileges (Select two)?

설명 Correct options:

Configure an Amazon S3 bucket to enable MFA (Multi Factor Authentication) delete

Close the company's AWS account

An IAM user with full administrator access can perform almost all AWS tasks except a few tasks designated only for the root account user. Some of the AWS tasks that only a root account user can do are as follows: change account name or root password or root email address, change AWS support plan, close AWS account, enable MFA on S3 bucket delete, create Cloudfront key pair, register for GovCloud. Even though the DevOps engineer is part of the admin group, he cannot configure an Amazon S3 bucket to enable MFA delete or close the company's AWS account.

Incorrect Options:

Delete the IAM user for his manager

Delete an S3 bucket from the production environment

Change the password for his own IAM user account

The DevOps engineer is part of the admin group, so he can delete any IAM user, delete the S3 bucket, and change the password for his own IAM user account.

For the complete list of AWS tasks that require AWS account root user credentials, please review this reference link:

https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html

질문 47: 정답

A multi-national company is looking at optimizing their AWS resources across various countries and regions. They want to understand the best practices on cost optimization, performance, and security for their system architecture spanning across multiple business units.

Which AWS service is the best fit for their requirements?

설명 Correct option:

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that draws upon best practices learned from AWS's aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and makes recommendations for saving money, improving system performance, or closing security gaps. It scans your AWS infrastructure and compares it to AWS Best practices in five categories (Cost Optimization, Performance, Security, Fault Tolerance, Service limits) and then provides recommendations.

How Trusted Advisor Works: via - https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

Incorrect options:

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. You can use Config to answer questions such as - "What did my AWS resource look like at xyz point in time?". It does not offer any feedback about architectural best practices.

AWS Management Console - The AWS Management Console is a web application that comprises and refers to a broad collection of service consoles for managing Amazon Web Services. You log into your AWS account using the AWS Management console. It does not offer any feedback about architectural best practices.

AWS Systems Manager - AWS Systems Manager is an AWS service that you can use to view and control your infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by

application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. It does not offer any feedback about architectural best practices.

Reference:

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

질문 48: 정답

While troubleshooting, a cloud architect realized that the Amazon EC2 instance is unable to connect to the internet using the Internet Gateway.

Which conditions should be met for internet connectivity to be established? (Select two)

설명 Correct options:

The network ACLs associated with the subnet must have rules to allow inbound and outbound traffic - The network access control lists (ACLs) that are associated with the subnet must have rules to allow inbound and outbound traffic on port 80 (for HTTP traffic) and port 443 (for HTTPs traffic). This is a necessary condition for Internet Gateway connectivity.

The route table in the instance's subnet should have a route to an Internet Gateway - A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed. The route table in the instance's subnet should have a route defined to the Internet Gateway.

Incorrect options:

The instance's subnet is not associated with any route table - This is an incorrect statement. A subnet is implicitly associated with the main route table if it is not explicitly associated with a particular route table. So, a subnet is always associated with some route table.

The instance's subnet is associated with multiple route tables with conflicting configurations - This is an incorrect statement. A subnet can only be associated with one route table at a time.

The subnet has been configured to be public and has no access to internet - This is an incorrect statement. Public subnets have access to the internet via Internet Gateway.

Reference:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

질문 49: 오답

An Internet-of-Things (IoT) company is planning on distributing a master sensor in people's homes to measure the key metrics from its smart devices. In order to provide adjustment commands for these devices, the company would like to have a streaming system that supports ordered data based on the sensor's key, and also sustains high throughput messages (thousands of messages per second).

As a solutions architect, which of the following AWS services would you recommend for this use-case?

설명 Correct option:

Amazon Kinesis Data Streams (KDS) - Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream.

However, there are certain limits you should keep in mind while using Amazon Kinesis Data Streams:

A Kinesis data stream stores records from 24 hours by default, up to 8760 hours (365 days).

The maximum size of a data blob (the data payload before Base64-encoding) within one record is 1 megabyte (MB). Each shard can support up to 1000 PUT records per second.

Kinesis is the right answer here, as by providing a partition key in your message, you can guarantee ordered messages for a specific sensor, even if your stream is sharded.

Incorrect options:

Amazon Simple Queue Service (SQS) - 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. Kinesis is better for streaming data since queues aren't meant for real-time streaming of data.

Amazon Simple Notification Service (SNS) - Amazon Simple Notification Service (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 SNS provides topics for high-throughput, push-based, many-to-many messaging. SNS cannot be used for data streaming. Therefore this option is not the best fit for the given use-case.

AWS Lambda - AWS Lambda lets you run code without provisioning or managing servers. It cannot be used for production-grade serverless log analytics. Lambda isn't meant to retain data either. Therefore this option is not the best fit for the given use-case.

Reference:

https://aws.amazon.com/kinesis/data-streams/faqs/

질문 50: 오답

A financial services firm uses a high-frequency trading system and wants to write the log files into Amazon S3. The system will also read these log files in parallel on a near real-time basis. The engineering team wants to address any data discrepancies that might arise when the trading system overwrites an existing log file and then tries to read that specific log file.

Which of the following options BEST describes the capabilities of Amazon S3 relevant to this scenario?

설명 Correct option:

A process replaces an existing object and immediately tries to read it. Amazon S3 always returns the latest version of the object

Amazon S3 delivers strong read-after-write consistency automatically, without changes to performance or availability, without sacrificing regional isolation for applications, and at no additional cost.

After a successful write of a new object or an overwrite of an existing object, any subsequent read request immediately receives the latest version of the object. S3 also provides strong consistency for list operations, so after a write, you can immediately perform a listing of the objects in a bucket with any changes reflected.

Strong read-after-write consistency helps when you need to immediately read an object after a write. For example, strong read-after-write consistency when you often read and list immediately after writing objects.

To summarize, all S3 GET, PUT, and LIST operations, as well as operations that change object tags, ACLs, or metadata, are strongly consistent. What you write is what you will read, and the results of a LIST will be an accurate reflection of what’s in the bucket.

Incorrect options:

A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the previous data

A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 does not return any data

A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the new data

These three options contradict the earlier details provided in the explanation.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#ConsistencyModel

https://aws.amazon.com/s3/faqs/

질문 51: 오답

A startup has created a cost-effective backup solution in another AWS Region. The application is running in warm standby mode and has Application Load Balancer (ALB) to support it from the front. The current failover process is manual and requires updating the DNS alias record to point to the secondary ALB in another Region in case of failure of the primary ALB.

As a Solutions Architect, what will you recommend to automate the failover process?

설명 Correct option:

Enable an Amazon Route 53 health check - Determining the health of an ELB endpoint is more complex than health checking a single IP address. For example, what if your application is running fine on EC2, but the load balancer itself isn't reachable? Or if your load balancer and your EC2 instances are working

correctly, but a bug in your code causes your application to crash? Or how about if the EC2 instances in one Availability Zone of a multi-AZ ELB are experiencing problems?

Route 53 DNS Failover handles all of these failure scenarios by integrating with ELB behind the scenes. Once enabled, Route 53 automatically configures and manages health checks for individual ELB nodes. Route 53 also takes advantage of the EC2 instance health checking that ELB performs (information on configuring your ELB health checks is available here). By combining the results of health checks of your EC2 instances and your ELBs, Route 53 DNS Failover can evaluate the health of the load balancer and the health of the application running on the EC2 instances behind it. In other words, if any part of the stack goes down, Route 53 detects the failure and routes traffic away from the failed endpoint.

Using Route 53 DNS Failover, you can run your primary application simultaneously in multiple AWS regions around the world and failover across regions. Your end-users will be routed to the closest (by latency), healthy region for your application. Route 53 automatically removes from service any region where your application is unavailable - it will pull an endpoint out of service if there is region-wide connectivity or operational issue, if your application goes down in that region, or if your ELB or EC2 instances go down in that region.

Incorrect options:

Enable an ALB health check - ELB health check verifies that a specified TCP port on an instance is accepting connections or a specified page has returned an error code of 200. It is not useful for the given failover scenario.

Enable an EC2 instance health check - Instance status checks monitor the software and network configuration of your instance. It is not intelligent enough to understand if the application on the instance is working correctly. Hence, this is not the right choice for the given use-case.

Configure Trusted Advisor to check on unhealthy instances - AWS Trusted Advisor examines the health check configuration for Auto Scaling groups. If Elastic Load Balancing is being used for an Auto Scaling group, the recommended configuration is to enable an Elastic Load Balancing health check. Trusted Advisor recommends certain configuration changes by comparing your system configurations to AWS Best practices. It cannot handle a failover the way Route 53 does.

References:

https://aws.amazon.com/blogs/aws/amazon-route-53-elb-integration-dns-failover/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/best-practice-checklist/

질문 52: 정답

A pharmaceutical company is considering moving to AWS Cloud to accelerate the research and development process. Most of the daily workflows would be centered around running batch jobs on EC2 instances with storage on EBS volumes. The CTO is concerned about meeting HIPAA compliance norms for sensitive data stored on EBS.

Which of the following options outline the correct capabilities of an encrypted EBS volume? (Select three)

설명 Correct options:

Data at rest inside the volume is encrypted

Any snapshot created from the volume is encrypted

Data moving between the volume and the instance is encrypted

Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with EC2 instances. When you create an encrypted EBS volume and attach it to a supported instance type, data stored at rest on the volume, data moving between the volume and the instance, snapshots created from the volume and volumes created from those snapshots are all encrypted. It uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and 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.

Therefore, the incorrect options are:

Data moving between the volume and the instance is NOT encrypted

Any snapshot created from the volume is NOT encrypted

Data at rest inside the volume is NOT encrypted

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

질문 53: 정답

You have just terminated an instance in the us-west-1a availability zone. The attached EBS volume is now available for attachment to other instances. An intern launches a new Linux EC2 instance in the us-west-1b availability zone and is attempting to attach the EBS volume. The intern informs you that it is not possible and needs your help.

Which of the following explanations would you provide to them?

설명 Correct option:

EBS volumes are AZ locked

An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive. EBS volumes are flexible. For current-generation volumes attached to current-generation instance types, you can dynamically increase size, modify the provisioned IOPS capacity, and change volume type on live production volumes.

When you create an EBS volume, it is automatically replicated within its Availability Zone to prevent data loss due to the failure of any single hardware component. You can attach an EBS volume to an EC2 instance in the same Availability Zone.

Incorrect options:

EBS volumes are region locked - It's confined to an Availability Zone and not by region.

The required IAM permissions are missing - This is a possibility as well but if permissions are not an issue then you are still confined to an availability zone.

The EBS volume is encrypted - This doesn't affect the ability to attach an EBS volume.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html

질문 55: 오답

The infrastructure team at a company maintains 5 different VPCs (let's call these VPCs A, B, C, D, E) for resource isolation. Due to the changed organizational structure, the team wants to interconnect all VPCs together. To facilitate this, the team has set up VPC peering connections between VPC A and all other VPCs in a hub and spoke model with VPC A at the center. However, the team has still failed to establish connectivity between all VPCs.

As a solutions architect, which of the following would you recommend as the MOST resource-efficient and scalable solution?

설명 Correct option:

Use a transit gateway to interconnect the VPCs

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

Transit Gateway Overview: via - https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Transitive Peering does not work for VPC peering connections. So, if you have a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and between VPC A and VPC C (pcx-aaaacccc). Then, there is no VPC peering connection between VPC B and VPC C. Instead of using VPC peering, you can use an AWS Transit Gateway that acts as a network transit hub, to interconnect your VPCs or connect your VPCs with on-premises networks. Therefore this is the correct option.

VPC Peering Connections Overview: via - https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.html

Incorrect options:

Use an internet gateway to interconnect the VPCs - An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic. You cannot use an internet gateway to interconnect your VPCs and on-premises networks, hence this option is incorrect.

Use a VPC endpoint to interconnect the VPCs - 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. You cannot use a VPC endpoint to interconnect your VPCs and on-premises networks, hence this option is incorrect.

Establish VPC peering connections between all VPCs - Establishing VPC peering between all VPCs is an inelegant and clumsy way to establish connectivity between all VPCs. Instead, you should use a Transit Gateway that acts as a network transit hub to interconnect your VPCs and on-premises networks.

References:

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html

질문 56: 오답

A gaming company is doing pre-launch testing for its new product. The company runs its production database on an Aurora MySQL DB cluster and the performance testing team wants access to multiple test databases that must be re-created from production data. The company has hired you as an AWS Certified Solutions Architect Associate to deploy a solution to create these test databases quickly with the LEAST required effort.

What would you suggest to address this use case?

설명 Correct option:

Use database cloning to create multiple clones of the production DB and use each clone as a test DB

You can quickly create clones of an Aurora DB by using the database cloning feature. In addition, database cloning uses a copy-on-write protocol, in which data is copied only at the time the data changes, either on the source database or the clone database. Cloning is much faster than a manual snapshot of the DB cluster.

For the given use case, the most optimal solution is to clone the DB cluster. This would allow the performance testing team to have quick access to the production data in an isolated way. The team can iterate over the various test phases by deleting existing test databases and then cloning the production DB to create new test DBs.

You cannot clone databases across AWS regions. The clone databases must be created in the same region as the source databases. Currently, you are limited to 15 clones based on a copy, including clones based on other clones. After that, only copies can be created. However, each copy can also have up to 15 clones.

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html

Incorrect options:

Enable database Backtracking on the production DB and let the testing team use the production DB - Using Backtracking, you can "rewind" the DB cluster to any time you specify. One of the major advantages of backtracking is that it can rewind the DB cluster much faster compared to restoring a DB cluster via point-

in-time restore (PITR) or via a manual DB cluster snapshot, which can take hours. Backtracking a DB cluster doesn't require a new DB cluster and rewinds the DB cluster in minutes.

However, as the given use-case is around pre-release testing, it does not make sense to use production DB itself for testing even if backtracking is enabled. The right solution is to use clones of the production DB for testing.

via - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Backtrack.html

Take a backup of the Aurora MySQL DB instance using the mysqldump utility, create multiple new test DB instances and restore each test DB from the backup - As the use-case mandates the least effort for database administration, therefore this option is not correct since using the mysqldump utility requires several manual steps to take a backup of a DB and restore into another DB.

Create additional Read Replicas of the Aurora MySQL production DB and use the Read Replicas for testing by promoting each Replica to be its own independent standalone instance - This option has been added as a distractor as you cannot promote an Aurora Read Replica to a standalone DB instance.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Backtrack.html

질문 59: 정답

A DevOps engineer at an organization is debugging issues related to an Amazon EC2 instance. The engineer has SSH'ed into the instance and he needs to retrieve the instance public IP from within a shell script running on the instance command line.

Can you identify the correct URL path to get the instance public IP?

설명 Correct option:

http://169.254.169.254/latest/meta-data/public-ipv4

Instance metadata is the data about your instance that you can use to configure or manage the running instance.

Instance user data is the data that you specified in the form of a configuration script while launching your instance.

The following URL paths can be used to get the instance meta data and user data from within the instance: http://169.254.169.254/latest/meta-data/

http://169.254.169.254/latest/user-data/

Further, you can get the instance public IP via the URL - http://169.254.169.254/latest/meta-data/public-ipv4

Incorrect options:

http://169.254.169.254/latest/user-data/public-ipv4

http://254.169.254.169/latest/meta-data/public-ipv4

http://254.169.254.169/latest/user-data/public-ipv4

These three options do not meet the specification for the URL path to get the instance public IP, so these are incorrect.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-add-user-data.html

질문 60: 정답

An online gaming company wants to block access to its application from specific countries; however, the company wants to allow its remote development team (from one of the blocked countries) to have access to the application. The application is deployed on EC2 instances running under an Application Load Balancer (ALB) with AWS WAF.

As a solutions architect, which of the following solutions can be combined to address the given use-case? (Select two)

설명 Correct options:

Use WAF geo match statement listing the countries that you want to block

Use WAF IP set statement that specifies the IP addresses that you want to allow through

AWS WAF is 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 WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns and rules that filter out specific traffic patterns you define.

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, or Amazon API Gateway for your APIs.

AWS WAF - How it Works via - https://aws.amazon.com/waf/

To block specific countries, you can create a WAF geo match statement listing the countries that you want to block, and to allow traffic from IPs of the remote development team, you can create a WAF IP set statement that specifies the IP addresses that you want to allow through. You can combine the two rules as shown below:

Incorrect options:

Create a deny rule for the blocked countries in the NACL associated to each of the EC2 instances - 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. NACL does not have the capability to block traffic based on geographic match conditions.

Use ALB geo match statement listing the countries that you want to block

Use ALB IP set statement that specifies the IP addresses that you want to allow through

An Application Load Balancer (ALB) operates at the request level (layer 7), routing traffic to targets – EC2 instances, containers, IP addresses, and Lambda functions based on the content of the request. Ideal for advanced load balancing of HTTP and HTTPS traffic, Application Load Balancer provides advanced request routing targeted at delivery of modern application architectures, including microservices and container-based applications.

An ALB cannot block or allow traffic based on geographic match conditions or IP based conditions. Both these options have been added as distractors.

References:

https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html

https://aws.amazon.com/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/

질문 62: 오답

A pharma company is working on developing a vaccine for the COVID-19 virus. The researchers at the company want to process the reference healthcare data in a highly available as well as HIPAA compliant in-memory database that supports caching results of SQL queries.

As a solutions architect, which of the following AWS services would you recommend for this task?

설명 Correct option:

ElastiCache for Redis/Memcached

ElastiCache Overview: via - https://aws.amazon.com/elasticache/redis-vs-memcached/

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Amazon ElastiCache for Redis is a great choice for real-time transactional and analytical processing use cases such as caching, chat/messaging, gaming leaderboards, geospatial, machine learning, media streaming, queues, real-time analytics, and session store. ElastiCache for Redis supports replication, high availability, and cluster sharding right out of the box.

Amazon ElastiCache for Memcached is a Memcached-compatible in-memory key-value store service that can be used as a cache or a data store. Amazon ElastiCache for Memcached is a great choice for implementing an in-memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL database. Session stores are easy to create with Amazon ElastiCache for Memcached.

Both ElastiCache for Redis and ElastiCache for Memcached are HIPAA Eligible. Therefore, this is the correct option.

Exam Alert:

Please review this comparison sheet for Redis vs Memcached features: via - https://aws.amazon.com/elasticache/redis-vs-memcached/

Incorrect Options:

DynamoDB Accelerator (DAX) - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. DAX does not support SQL query caching.

DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore, and in-memory caching (via DAX) for internet-scale applications. DynamoDB is not an in-memory database, so this option is incorrect.

DocumentDB - Amazon DocumentDB is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data. DocumentDB is not an in-memory database, so this option is incorrect.

References:

https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-elasticache-for-redis-is-now-hipaa-eligible-to-help-you-power-secure-healthcare-applications-with-sub-millisecond-latency/

https://aws.amazon.com/elasticache/redis/

https://aws.amazon.com/about-aws/whats-new/2022/08/amazon-elasticache-memcached-hipaa-eligible/

https://aws.amazon.com/blogs/database/automating-sql-caching-for-amazon-elasticache-and-amazon-rds/

질문 63: 정답

A company wants to store business-critical data on EBS volumes which provide persistent storage independent of EC2 instances. During a test run, the development team found that on terminating an EC2 instance, the attached EBS volume was also lost, which was contrary to their assumptions.

As a solutions architect, could you explain this issue?

설명 Correct option:

The EBS volume was configured as the root volume of the Amazon EC2 instance. On termination of the instance, the default behavior is to also terminate the attached root volume

Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale.

When you launch an instance, the root device volume contains the image used to boot the instance. You can choose between AMIs backed by Amazon EC2 instance store and AMIs backed by Amazon EBS.

By default, the root volume for an AMI backed by Amazon EBS is deleted when the instance terminates. You can change the default behavior to ensure that the volume persists after the instance terminates. Non-root EBS volumes remain available even after you terminate an instance to which the volumes were attached. Therefore, this option is correct.

Incorrect options:

The EBS volumes were not backed up on Amazon S3 storage, resulting in the loss of volume

The EBS volumes were not backed up on EFS file system storage, resulting in the loss of volume

EBS volumes do not need to back up the data on Amazon S3 or EFS filesystem. Both these options are added as distractors.

On termination of an EC2 instance, all the attached EBS volumes are always terminated - As mentioned earlier, non-root EBS volumes remain available even after you terminate an instance to which the volumes were attached. Hence this option is incorrect.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html

질문 64: 오답

An application hosted on Amazon EC2 contains sensitive personal information about all its customers and needs to be protected from all types of cyber-attacks. The company is considering using the AWS Web Application Firewall (WAF) to handle this requirement.

Can you identify the correct solution leveraging the capabilities of WAF?

설명 Correct option:

Create a CloudFront distribution for the application on Amazon EC2 instances. Deploy AWS WAF on Amazon CloudFront to provide the necessary safety measures

When you use AWS WAF with CloudFront, you can protect your applications running on any HTTP webserver, whether it's a webserver that's running in Amazon Elastic Compute Cloud (Amazon EC2) or a web server that you manage privately. You can also configure CloudFront to require HTTPS between CloudFront and your own webserver, as well as between viewers and CloudFront.

AWS WAF is tightly integrated with Amazon CloudFront and the Application Load Balancer (ALB), services that AWS customers commonly use to deliver content for their websites and applications. When you use AWS WAF on Amazon CloudFront, your rules run in all AWS Edge Locations, located around the world close to your end-users. This means security doesn't come at the expense of performance. Blocked requests are stopped before they reach your web servers. When you use AWS WAF on Application Load Balancer, your rules run in the region and can be used to protect internet-facing as well as internal load balancers.

Incorrect options:

Configure an Application Load Balancer (ALB) to balance the workload for all the EC2 instances. Configure CloudFront to distribute from an ALB since WAF cannot be directly configured on ALBs. This configuration

not only provides necessary safety but is scalable too - This statement is wrong. You can configure WAF on Application Load Balancers (ALB).

AWS WAF can be directly configured on Amazon EC2 instances for ensuring the security of the underlying application data* - AWS WAF can be deployed on Amazon CloudFront, the Application Load Balancer (ALB), and Amazon API Gateway. It cannot be configured directly on an EC2 instance.

AWS WAF can be directly configured only on an Application Load Balancer (ALB) or an Amazon API Gateway. One of these two services can then be configured with Amazon EC2 to build the needed secure architecture - This statement is only partially correct. WAF can also be deployed on Amazon CloudFront service.

References:

https://aws.amazon.com/waf/faqs/

https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html

질문 65: 정답

Which of the following is true regarding cross-zone load balancing as seen in Application Load Balancer versus Network Load Balancer?

설명 Correct option:

By default, cross-zone load balancing is enabled for Application Load Balancer and disabled for Network Load Balancer

By default, cross-zone load balancing is enabled for Application Load Balancer and disabled for Network Load Balancer. When cross-zone load balancing is enabled, each load balancer node distributes traffic across the registered targets in all the enabled Availability Zones. When cross-zone load balancing is disabled, each load balancer node distributes traffic only across the registered targets in its Availability Zone.

How cross-zone load balancing works: via - https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html

Incorrect Options:

By default, cross-zone load balancing is disabled for both Application Load Balancer and Network Load Balancer

By default, cross-zone load balancing is enabled for both Application Load Balancer and Network Load Balancer

By default, cross-zone load balancing is disabled for Application Load Balancer and enabled for Network Load Balancer

Per the default cross-zone load balancing settings described earlier in the explanation, these three options are incorrect.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html