



Amazon-Web-Services

Exam Questions SAA-C03

AWS Certified Solutions Architect - Associate (SAA-C03)

NEW QUESTION 1

- (Topic 1)

A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.

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

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

Answer: A

Explanation:

AWS Fargate is a serverless compute engine that lets users run containers without having to manage servers or clusters of Amazon EC2 instances¹. Users can use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Amazon ECS is a fully managed container orchestration service that supports both Docker and Kubernetes². Service Auto Scaling is a feature that allows users to adjust the desired number of tasks in an ECS service based on CloudWatch metrics, such as CPU utilization or request count³. Users can use AWS Fargate on Amazon ECS to migrate the application to AWS with minimum code changes and minimum development effort, as they only need to package their application in containers and specify the CPU and memory requirements.

Users can also use an Application Load Balancer to distribute the incoming requests. An Application Load Balancer is a load balancer that operates at the application layer and routes traffic to targets based on the content of the request. Users can register their ECS tasks as targets for an Application Load Balancer and configure listener rules to route requests to different target groups based on path or host headers. Users can use an Application Load Balancer to improve the availability and performance of their web application.

NEW QUESTION 2

- (Topic 1)

A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions

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

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

Answer: A

Explanation:

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>

NEW QUESTION 3

- (Topic 1)

A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.

What should a solutions architect do to meet these requirements?

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft> <https://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html>

NEW QUESTION 4

- (Topic 1)

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB Set up a rule in DynamoDB to remove sensitive data from every transaction upon write Use DynamoDB Streams to share the transactions data with other applications
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3 Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data
- C. Other applications can consume the data stored in Amazon S3
- D. Stream the transactions data into Amazon Kinesis Data Streams Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB Other applications can consume the transactions data off the Kinesis data stream.
- E. Store the batched transactions data in Amazon S3 as file
- F. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3 The Lambda function then stores the data in Amazon DynamoDB Other applications can consume transaction files stored in Amazon S3.

Answer: C

Explanation:

The destination of your Kinesis Data Firehose delivery stream. Kinesis Data Firehose can send data records to various destinations, including Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service, and any HTTP endpoint that is owned by you or any of your third-party service providers. The following are the supported destinations:

- * Amazon OpenSearch Service
- * Amazon S3
- * Datadog
- * Dynatrace
- * Honeycomb
- * HTTP Endpoint
- * Logic Monitor
- * MongoDB Cloud
- * New Relic
- * Splunk
- * Sumo Logic <https://docs.aws.amazon.com/firehose/latest/dev/create-name.html>

<https://aws.amazon.com/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.

NEW QUESTION 5

- (Topic 1)

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

- A. Create an Auto Scaling group so that EC2 instances can scale out
- B. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- C. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket
- D. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data
- F. Configure the S3 bucket as the rule's target
- G. Create a second EventBridge (CloudWatch Events) rule to send events when the upload to the S3 bucket is complete
- H. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
- I. Create a Docker container to use instead of an EC2 instance
- J. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Answer: B

Explanation:

Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks.

<https://aws.amazon.com/appflow/>

NEW QUESTION 6

- (Topic 1)

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

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

Answer: B

Explanation:

https://aws.amazon.com/s3/storage-classes/?trk=66264cd8-3b73-416c-9693-ea7cf4fe846a&sc_channel=ps&s_kwid=AL1442213!536452716950!p!!g!!aws%20s3%20pricing&ef_id=Cj0KCQjwnbmaBhD-ARIsAGTPcfVHUZN5_BMrzl5zBcaC8KnqpnNZvbZzqPkH6k7q4JcYO5KFLx0YYgaAm6nEALw_wC6G:s&s_kwid=AL1442213!536452716950!p!!g!!aws%20s3%20pricing

NEW QUESTION 7

- (Topic 1)

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

- A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
- B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
- C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
- D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Answer: B

Explanation:

AWS Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your

costs. <https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html>

NEW QUESTION 8

- (Topic 1)

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices. The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

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

Answer: D

Explanation:

<https://aws.amazon.com/sqs/features/>

By routing incoming requests to Amazon SQS, the company can decouple the job requests from the processing instances. This allows them to scale the number of instances based on the size of the queue, providing more resources when needed. Additionally, using an Auto Scaling group based on the queue size will automatically scale the number of instances up or down depending on the workload. Updating the software to read from the queue will allow it to process the job requests in a more efficient manner, improving the performance of the system.

NEW QUESTION 9

- (Topic 1)

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day. What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Stream.
- E. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Answer: D

Explanation:

<https://aws.amazon.com/es/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/>

NEW QUESTION 10

- (Topic 1)

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

What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

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

Answer: A

Explanation:

In this scenario, the company wants to avoid regional data transfer charges while downloading and uploading images from Amazon S3. To accomplish this at the lowest cost, the NAT gateway should be launched in each availability zone that the EC2 instances are running in. This allows the EC2 instances to route traffic through the local NAT gateway instead of sending traffic across an availability zone boundary and incurring regional data transfer fees. This method will help reduce the data transfer costs since inter- Availability Zone data transfers in a single region are free of charge.

Reference:

AWS NAT Gateway documentation: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

NEW QUESTION 10

- (Topic 1)

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

Which solution meets these requirements?

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

Answer: B

Explanation:

To address the issue of bandwidth limitations on the company's on-premises application, and to minimize the impact on internal user connectivity, a new AWS Direct Connect connection should be established to direct backup traffic through this new connection. This solution will offer a secure, high-speed connection between the company's data center and AWS, which will allow the company to transfer data quickly without consuming internet bandwidth.

Reference:

AWS Direct Connect documentation: <https://aws.amazon.com/directconnect/>

NEW QUESTION 15

- (Topic 1)

A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.

What should a solutions architect do to meet these requirements?

- A. Move the catalog to Amazon ElastiCache for Redis.
- B. Deploy a larger EC2 instance with a larger instance store.
- C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
- D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Answer: D

Explanation:

Moving the catalog to an Amazon Elastic File System (Amazon EFS) file system provides both high availability and durability. Amazon EFS is a fully-managed, highly-available, and durable file system that is built to scale on demand. With Amazon EFS, the catalog data can be stored and accessed from multiple EC2 instances in different availability zones, ensuring high availability. Also, Amazon EFS automatically stores files redundantly within and across multiple availability zones, making it a durable storage option.

NEW QUESTION 17

- (Topic 1)

A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

- A. Stop the DB instance when tests are complete
- B. Restart the DB instance when required.
- C. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
- D. Create a snapshot when tests are complete
- E. Terminate the DB instance and restore the snapshot when required.
- F. Modify the DB instance to a low-capacity instance when tests are complete
- G. Modify the DB instance again when required.

Answer: A

Explanation:

To reduce the cost of running the tests without reducing the compute and memory attributes of the Amazon RDS for MySQL DB instance, the development team can stop the instance when tests are completed and restart it when required. Stopping the DB instance when not in use can help save costs because customers are only charged for storage while the DB instance is stopped. During this time, automated backups and automated DB instance maintenance are suspended. When the instance is restarted, it retains the same configurations, security groups, and DB parameter groups as when it was stopped.

Reference:

Amazon RDS Documentation: Stopping and Starting a DB instance (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html)

NEW QUESTION 18

- (Topic 1)

A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

- A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval
- B. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
- C. Store individual files in Amazon S3 Intelligent-Tiering
- D. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year
- E. Query and retrieve the files that are in Amazon S3 by using Amazon Athena
- F. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
- G. Store individual files with tags in Amazon S3 Standard storage
- H. Store search metadata for each archive in Amazon S3 Standard storage
- I. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year
- J. Query and retrieve the files by searching for metadata from Amazon S3.
- K. Store individual files in Amazon S3 Standard storage
- L. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year
- M. Store search metadata in Amazon S3
- N. Query the files from Amazon S3
- O. Retrieve the files from S3 Glacier Deep Archive.

Answer: B

Explanation:

"For archive data that needs immediate access, such as medical images, news media assets, or genomics data, choose the S3 Glacier Instant Retrieval storage class, an archive storage class that delivers the lowest cost storage with milliseconds retrieval. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, choose S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5- 12 hours." <https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-s3-glacier-instant-retrieval-storage-class/>

NEW QUESTION 22

- (Topic 1)

A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability. What should a solutions architect do to meet these requirements?

- A. Create an AWS Lambda function to apply the patch to all EC2 instances.
- B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
- C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
- D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Answer: B

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/about-windows-app-patching.html>

NEW QUESTION 26

- (Topic 1)

A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources. What should a solutions architect do to meet these requirements?

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

Answer: B

Explanation:

AWS Config is a fully managed service that allows the company to assess, audit, and evaluate the configurations of its AWS resources. It provides a detailed inventory of the resources in use and tracks changes to resource configurations. AWS Config can detect configuration changes and alert the company when changes occur. It also provides a historical view of changes, which is essential for compliance and governance purposes. AWS CloudTrail is a fully managed service that provides a detailed history of API calls made to the company's AWS resources. It records all API activity in the AWS account, including who made the API call, when the call was made, and what resources were affected by the call. This information is critical for security and auditing purposes, as it allows the company to investigate any suspicious activity that might occur on its AWS resources.

NEW QUESTION 27

- (Topic 1)

A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.

The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.

A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay. Which solution meets these requirements?

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

Answer: B

Explanation:

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

NEW QUESTION 28

- (Topic 1)

A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions.

The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

- A. Deploy a Network Load Balancer (NLB) and an associated target group
- B. Associate the target group with the Auto Scaling group
- C. Use the NLB as an AWS Global Accelerator endpoint in each Region.
- D. Deploy an Application Load Balancer (ALB) and an associated target group
- E. Associate the target group with the Auto Scaling group
- F. Use the ALB as an AWS Global Accelerator endpoint in each Region.
- G. Deploy a Network Load Balancer (NLB) and an associated target group
- H. Associate the target group with the Auto Scaling group
- I. Create an Amazon Route 53 latency record that points to aliases for each NL
- J. Create an Amazon CloudFront distribution that uses the latency record as an origin.
- K. Deploy an Application Load Balancer (ALB) and an associated target group
- L. Associate the target group with the Auto Scaling group
- M. Create an Amazon Route 53 weighted record that points to aliases for each AL
- N. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Answer: D

Explanation:

<https://aws.amazon.com/global-accelerator/faqs/>

HTTP /HTTPS - ALB ; TCP and UDP - NLB; Lowest latency routing and more throughput. Also supports failover, uses Anycast Ip addressing - Global Accelerator Caching at Edge Locations – Cloudfront

WS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint..

NEW QUESTION 31

- (Topic 1)

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

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

Answer: D

Explanation:

<https://aws.amazon.com/shield/faqs/>

NEW QUESTION 32

- (Topic 1)

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NL
- B. supplying the URL of the company's application.
- C. Add a cron job to the EC2 instances to check the local application's logs once each minute
- D. If HTTP errors are detected, the application will restart.
- E. Replace the NLB with an Application Load Balance
- F. Enable HTTP health checks by supplying the URL of the company's application
- G. Configure an Auto Scaling action to replace unhealthy instances.
- H. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NL
- I. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Answer: C

Explanation:

Application availability: NLB cannot assure the availability of the application. This is because it bases its decisions solely on network and TCP-layer variables and has no awareness of the application at all. Generally, NLB determines availability based on the ability of a server to respond to ICMP ping or to correctly complete the three-way TCP handshake. ALB goes much deeper and is capable of determining availability based on not only a successful HTTP GET of a particular page but also the verification that the content is as was expected based on the input parameters.

NEW QUESTION 36

- (Topic 1)

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet those requirements?

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

Answer: C

Explanation:

using AWS ECS on AWS Fargate since they requirements are for scalability and availability without having to provision and manage the underlying infrastructure to run the containerized workload. <https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html>

NEW QUESTION 41

- (Topic 1)

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.

A solutions architect needs to design a solution that stores customer data that is created during database upgrades.

Which solution will meet these requirements?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage.
- D. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- E. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Answer: D

Explanation:

<https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/>

RDS proxy can improve application availability in such a situation by waiting for the new database instance to be functional and maintaining any requests received from the application during this time. The end result is that the application is more resilient to issues with the underlying database.

This will enable solution to hold data till the time DB comes back to normal. RDS proxy is to optimally utilize the connection between Lambda and DB. Lambda can open multiple connections concurrently which can be taxing on DB compute resources, hence RDS proxy was introduced to manage and leverage these connections efficiently.

NEW QUESTION 43

- (Topic 1)

A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received.

Which solution will meet these requirements?

- A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order.
- B. Subscribe an AWS Lambda function to the topic to perform processing.
- C. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order.
- D. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
- E. Use an API Gateway authorizer to block any requests while the application processes an order.
- F. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order.
- G. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Answer: B

Explanation:

To ensure that orders are processed in the order that they are received, the best solution is to use an Amazon SQS FIFO (First-In-First-Out) queue. This type of queue maintains the exact order in which messages are sent and received. In this case, the application can send information about new orders to an Amazon API Gateway REST API, which can then use an API Gateway integration to send a message to an Amazon SQS FIFO queue for processing. The queue can then be configured to invoke an AWS Lambda function to perform the necessary processing on each order. This ensures that orders are processed in the exact order in which they are received.

NEW QUESTION 47

- (Topic 1)

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

Which solution will meet these requirements?

- A. Share the dashboard from the CloudWatch console.
- B. Enter the product manager's email address, and complete the sharing step.
- C. Provide a shareable link for the dashboard to the product manager.
- D. Create an IAM user specifically for the product manager.
- E. Attach the CloudWatch Read Only Access managed policy to the user.
- F. Share the new login credential with the product manager.

- G. Share the browser URL of the correct dashboard with the product manager.
- H. Create an IAM user for the company's employees, Attach the View Only Access AWS managed policy to the IAM use
- I. Share the new login credentials with the product manager
- J. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
- K. Deploy a bastion server in a public subnet
- L. When the product manager requires access to the dashboard, start the server and share the RDP credential
- M. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Answer: B

Explanation:

To provide the product manager access to the Amazon CloudWatch dashboard while following the principle of least privilege, a solution architect should create an IAM user specifically for the product manager and attach the CloudWatch Read Only Access managed policy to the user. This policy allows the user to view the dashboard without being able to make any changes to it. The solution architect should then share the new login credential with the product manager and provide them with the browser URL of the correct dashboard.

NEW QUESTION 50

- (Topic 1)

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

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

Answer: C

NEW QUESTION 52

- (Topic 1)

A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access. Which solution will meet these requirements?

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

Answer: B

Explanation:

Amazon QuickSight is a data visualization service that allows you to create interactive dashboards and reports from various data sources, including Amazon S3 and Amazon RDS for PostgreSQL. You can connect all the data sources and create new datasets in QuickSight, and then publish dashboards to visualize the data. You can also share the dashboards with the appropriate users and groups, and control their access levels using IAM roles and permissions.

Reference: <https://docs.aws.amazon.com/quicksight/latest/user/working-with-data-sources.html>

NEW QUESTION 56

- (Topic 1)

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

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

NEW QUESTION 57

- (Topic 1)

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

Which solution will meet these requirements?

- A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default UR
- B. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- C. Create Route 53 DNS records with the company's domain nam
- D. Point the alias record to the Regional API Gateway stage endpoint
- E. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
- F. Create a Regional API Gateway endpoint
- G. Associate the API Gateway endpoint with the company's domain nam
- H. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Regio
- I. Attach the certificate to the API Gateway endpoint
- J. Configure Route 53 to route traffic to the API Gateway endpoint.
- K. Create a Regional API Gateway endpoint
- L. Associate the API Gateway endpoint with the company's domain nam
- M. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Regio
- N. Attach the certificate to the API Gateway API
- O. Create Route 53 DNS records with the company's domain nam
- P. Point an A record to the company's domain name.

Answer: C

Explanation:

To design the API Gateway URL with the company's domain name and corresponding certificate, the company needs to do the following: 1. Create a Regional API Gateway endpoint: This will allow the company to create an endpoint that is specific to a region. 2. Associate the API Gateway endpoint with the company's domain name: This will allow the company to use its own domain name for the API Gateway URL. 3. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region: This will allow the company to use HTTPS for secure communication with its APIs. 4. Attach the certificate to the API Gateway endpoint: This will allow the company to use the certificate for securing the API Gateway URL. 5. Configure Route 53 to route traffic to the API Gateway endpoint: This will allow the company to use Route 53 to route traffic to the API Gateway URL using the company's domain name.

NEW QUESTION 59

- (Topic 1)

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

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

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

Answer: D

Explanation:

The visibility timeout begins when Amazon SQS returns a message. During this time, the consumer processes and deletes the message. However, if the consumer fails before deleting the message and your system doesn't call the DeleteMessage action for that message before the visibility timeout expires, the message becomes visible to other consumers and the message is received again. If a message must be received only once, your consumer should delete it within the duration of the visibility timeout. <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

Keyword: SQS queue writes to an Amazon RDS. From this, Option D is the best choice; other options are ruled out [Option A - You can't introduce one more Queue in the existing one; Option B - only Permission; Option C - Only Retrieves Messages]. FIFO queues are designed to never introduce duplicate messages. However, your message producer might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval. For standard queues, you might occasionally receive a duplicate copy of a message (at-least- once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).

NEW QUESTION 61

- (Topic 1)

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

Which design should the solutions architect use?

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

Answer: C

Explanation:

"Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue"

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue. To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows: Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue

NEW QUESTION 65

- (Topic 1)

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

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

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

Answer: A

Explanation:

You might want to use Transfer Acceleration on a bucket for various reasons, including the following:

You have customers that upload to a centralized bucket from all over the world. You transfer gigabytes to terabytes of data on a regular basis across continents.

You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

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

[https://aws.amazon.com/s3/transfer-acceleration/#:~:text=S3%20Transfer%20Acceleration%20\(S3TA\)%20reduces,to%20S3%20for%20remote%20applications](https://aws.amazon.com/s3/transfer-acceleration/#:~:text=S3%20Transfer%20Acceleration%20(S3TA)%20reduces,to%20S3%20for%20remote%20applications):

"Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects.

Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet"

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html>

"Improved throughput - You can upload parts in parallel to improve throughput."

NEW QUESTION 66

- (Topic 1)

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses.

Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Select TWO.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization

Answer: AC

Explanation:

(<https://aws.amazon.com/cloudfront>)

NEW QUESTION 70

- (Topic 1)

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

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

Answer: A

Explanation:

"In some cases, this connection alone is not enough. It is always better to guarantee a fallback connection as the backup of DX. There are several options, but implementing it with an AWS Site-To-Site VPN is a real cost-effective solution that can be exploited to reduce costs or, in the meantime, wait for the setup of a

second DX." <https://www.proud2becloud.com/hybrid-cloud-networking-backup-aws-direct-connect-network-connection-with-aws-site-to-site-vpn/>

NEW QUESTION 73

- (Topic 1)

A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.

Which combination of steps should a solutions architect take to meet these requirements?

(Choose two.)

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Answer: AB

Explanation:

To protect data in an S3 bucket from accidental deletion, versioning should be enabled, which enables you to preserve, retrieve, and restore every version of every object in an S3 bucket. Additionally, enabling MFA (multi-factor authentication) Delete on the S3 bucket adds an extra layer of protection by requiring an authentication token in addition to the user's access keys to delete objects in the bucket.

Reference:

AWS S3 Versioning documentation: <https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

AWS S3 MFA Delete documentation: <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

NEW QUESTION 77

- (Topic 1)

A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

- A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificat
- B. Apply the certificate to the AL
- C. Use the managed renewal feature to automatically rotate the certificate.
- D. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificat
- E. Import the key material from the certificat
- F. Apply the certificate to the AL
- G. Use the managed renewal feature to automatically rotate the certificate.
- H. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root C
- I. Apply the certificate to the AL
- J. Use the managed renewal feature to automatically rotate the certificate.
- K. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificat
- L. Apply the certificate to the AL
- M. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiratio
- N. Rotate the certificate manually.

Answer: D

Explanation:

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

NEW QUESTION 80

- (Topic 1)

A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function.

Which solution meets these requirements?

- A. Add an execution role to the function with lambda: InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda: InvokeFunction as the action and Service:amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:* as the action and Service:events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda: InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Answer: D

Explanation:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policies-eventbridge.html#lambda-permissions>

NEW QUESTION 84

- (Topic 1)

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses a customer managed customer master key (CMK) to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

- A. Make the encrypted AMI and snapshots publicly availabl
- B. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key
- C. Modify the launchPermission property of the AM
- D. Share the AMI with the MSP Partner's AWS account onl
- E. Modify the CMK's key policy to allow the MSP Partner's AWS account to use the key.

- F. Modify the launchPermission property of the AMI Share the AMI with the MSP Partner's AWS account onl
- G. Modify the CMK's key policy to trust a new CMK that is owned by the MSP Partner for encryption.
- H. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS accoun
- I. Encrypt the S3 bucket with a CMK that is owned by the MSP Partner Copy and launch the AMI in the MSP Partner's AWS account.

Answer: B

Explanation:

Share the existing KMS key with the MSP external account because it has already been used to encrypt the AMI snapshot.
<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

NEW QUESTION 86

- (Topic 1)

A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud. Which solution will meet these requirements?

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

Answer: C

Explanation:

AWS Network Firewall supports both inspection and filtering as required

NEW QUESTION 87

- (Topic 1)

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database. Which solution meets these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR block
- B. Associate the route table to the database subnets.
- C. Create a security group that denies ingress from the security group used by instances in the public subnet
- D. Attach the security group to an Amazon RDS DB instance.
- E. Create a security group that allows ingress from the security group used by instances in the private subnet
- F. Attach the security group to an Amazon RDS DB instance.
- G. Create a new peering connection between the public subnets and the private subnet
- H. Create a different peering connection between the private subnets and the databasesubnets.

Answer: C

Explanation:

Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).
"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group." Source:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups

NEW QUESTION 89

- (Topic 1)

A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely. Which storage solution will meet these requirements MOST cost-effectively?

- A. Configure S3 Intelligent-Tiering to automatically migrate objects.
- B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
- C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
- D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

Answer: B

Explanation:

The storage solution that will meet these requirements most cost-effectively is B: Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month. Amazon S3 Glacier Deep Archive is a secure, durable, and extremely low-cost Amazon S3 storage class for long-term retention of data that is rarely accessed and for which retrieval times of several hours are acceptable. It is the lowest-cost storage option in Amazon S3, making it a cost-effective choice for storing backup files that are not accessed after 1 month. You can use an S3 Lifecycle configuration to automatically transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month. This will minimize the storage costs for the backup files that are not accessed frequently.

NEW QUESTION 93

- (Topic 1)

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

- A. Configure DynamoDB global table

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html>

NEW QUESTION 96

- (Topic 1)

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

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

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded,
- F. send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

Answer: AB

Explanation:

? Creating an Amazon Simple Queue Service (SQS) queue and configuring the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket will ensure that the Lambda function is triggered in a stateless and durable manner.

? Configuring the Lambda function to use the SQS queue as the invocation source, and deleting the message in the queue after it is successfully processed will ensure that the Lambda function processes the image in a stateless and durable manner.

Amazon 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. When new images are uploaded to the S3 bucket, SQS will trigger the Lambda function to process the image and compress it. Once the image is processed, the SQS message is deleted, ensuring that the Lambda function is stateless and durable.

NEW QUESTION 97

- (Topic 1)

A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.

Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data.
- B. Store the resulting JSON file in an Amazon Aurora DB cluster.
- C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue.
- D. Use Amazon EC2 instances to read from the queue and process the data.
- E. Store the resulting JSON file in Amazon DynamoDB.
- F. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue.
- G. Use an AWS Lambda function to read from the queue and process the data.
- H. Store the resulting JSON file in Amazon DynamoDB.
- I. Most Voted
- J. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded.
- K. Use an AWS Lambda function to consume the event from the stream and process the data.
- L. Store the resulting JSON file in Amazon Aurora DB cluster.

Answer: C

Explanation:

Amazon S3 sends event notifications about S3 buckets (for example, object created, object removed, or object restored) to an SNS topic in the same Region. The SNS topic publishes the event to an SQS queue in the central Region.

The SQS queue is configured as the event source for your Lambda function and buffers the event messages for the Lambda function.

The Lambda function polls the SQS queue for messages and processes the Amazon S3 event notifications according to your application's requirements.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/subscribe-a-lambda-function-to-event-notifications-from-s3-buckets-in-different-aws-regions.html>

NEW QUESTION 101

- (Topic 1)

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

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

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

Answer: A

Explanation:

<https://aws.amazon.com/about-aws/whats-new/2018/03/introducing-amazon-vpc-nat-gateway-in-the-aws-govcloud-us-region/#:~:text=NAT%20Gateway%20is%20a%20highly,instances%20in%20a%20private%20subnet.>
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

NEW QUESTION 104

- (Topic 1)

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

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html> <https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>

NEW QUESTION 108

- (Topic 1)

An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.
Which solution will provide private network connectivity to Amazon S3?

- A. Create a gateway VPC endpoint to the S3 bucket.
- B. Stream the logs to Amazon CloudWatch Log
- C. Export the logs to the S3 bucket.
- D. Create an instance profile on Amazon EC2 to allow S3 access.
- E. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Answer: A

Explanation:

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet

NEW QUESTION 113

- (Topic 1)

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.

During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.

Which solution will meet these requirements?

- A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instance
- B. Connect the database by using native Java Database Connectivity (JDBC) drivers.
- C. Change the platform from Aurora to Amazon DynamoD
- D. Provision a DynamoDB Accelerator (DAX) cluste
- E. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
- F. Set up two Lambda function
- G. Configure one function to receive the informatio
- H. Configure the other function to load the information into the databas
- I. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
- J. Set up two Lambda function
- K. Configure one function to receive the informatio
- L. Configure the other function to load the information into the databas
- M. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Answer: B

Explanation:

bottlenecks can be avoided with queues (SQS).

NEW QUESTION 117

- (Topic 1)

A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.

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

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

Answer: B

Explanation:

To achieve high availability with minimum downtime and minimum loss of data, the Auto Scaling group should be configured to use multiple Availability Zones to ensure that there is no single point of failure. The database should be configured as Multi-AZ to enable automatic failover in case of an outage in the primary Availability Zone. Additionally, an Amazon RDS Proxy instance can be used to improve the scalability and availability of the database by reducing connection failures and improving failover times.

NEW QUESTION 121

- (Topic 1)

A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.

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

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

Answer: C

Explanation:

To meet the requirements of the company to have access to both AWS and on-premises file storage with minimum latency, a hybrid cloud architecture can be used. One solution is to deploy and configure Amazon FSx for Windows File Server on AWS, which provides fully managed Windows file servers. The on-premises file data can be moved to the FSx File Gateway, which can act as a bridge between on-premises and AWS file storage. The cloud workloads can be configured to use FSx for Windows File Server on AWS, while the on-premises workloads can be configured to use the FSx File Gateway. This solution minimizes operational overhead and requires no significant changes to the existing file access patterns. The connectivity between on-premises and AWS can be established using an AWS Site-to-Site VPN connection.

Reference:

AWS FSx for Windows File Server: <https://aws.amazon.com/fsx/windows/> AWS FSx File Gateway: <https://aws.amazon.com/fsx/file-gateway/>

AWS Site-to-Site VPN: <https://aws.amazon.com/vpn/site-to-site-vpn/>

NEW QUESTION 124

- (Topic 1)

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

- A. Use Spot Instances for the production EC2 instance
- B. Use Reserved Instances for the development and test EC2 instances.
- C. Use Reserved Instances for the production EC2 instance
- D. Use On-Demand Instances for the development and test EC2 instances.
- E. Use Spot blocks for the production EC2 instance
- F. Use Reserved Instances for the development and test EC2 instances.
- G. Use On-Demand Instances for the production EC2 instance
- H. Use Spot blocks for the development and test EC2 instances.

Answer: B

NEW QUESTION 126

- (Topic 2)

A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

- A. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.
- B. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.
- C. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.
- D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

Answer: D

Explanation:

This solution meets the requirements of saving money on storage while keeping the most accessed files readily available for the users. S3 Lifecycle policy can automatically move objects from one storage class to another based on predefined rules. S3 Standard-IA is a lower-cost storage class for data that is accessed less frequently, but requires rapid access when needed. It is suitable for ringtones older than 90 days that are downloaded infrequently.

Option A is incorrect because configuring S3 Standard-IA for the initial storage tier of the objects can incur higher costs for frequent access and retrieval fees.

Option B is incorrect

because moving the files to S3 Intelligent-Tiering can incur additional monitoring and automation fees that may not be necessary for ringtones older than 90 days.

Option C is incorrect because using S3 inventory to manage objects and move them to S3 Standard-IA can be complex and time-consuming, and it does not provide automatic cost savings. References:

? <https://aws.amazon.com/s3/storage-classes/>

? <https://aws.amazon.com/s3/cloud-storage-cost-optimization-ebook/>

NEW QUESTION 130

- (Topic 2)

A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead.

Which solution will meet these requirements?

- A. Update the Route 53 records to use a latency routing policy
- B. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
- C. Set up a Route 53 active-passive failover configuration
- D. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- E. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoint
- F. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
- G. Update the Route 53 records to use a multivalue answer routing policy
- H. Create a health check
- I. Direct traffic to the website if the health check passes
- J. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

Answer: B

Explanation:

This solution meets the requirements of directing users to a backup static error page if the primary website is unavailable, minimizing changes and infrastructure overhead. Route 53 active-passive failover configuration can route traffic to a primary resource when it is healthy or to a secondary resource when the primary resource is unhealthy. Route 53 health checks can monitor the health of the ALB endpoint and trigger the failover when needed. The static error page can be hosted in an S3 bucket that is configured as a website, which is a simple and cost-effective way to serve static content.

Option A is incorrect because using a latency routing policy can route traffic based on the lowest network latency for users, but it does not provide failover functionality. Option C is incorrect because using an active-active configuration with the ALB and an EC2 instance can increase the infrastructure overhead and complexity, and it does not guarantee that the EC2 instance will always be healthy. Option D is incorrect because using a multivalue answer routing policy can return multiple values for a query, but it does not provide failover functionality.

References:

? <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-failover.html>

? <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html>

? <https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

NEW QUESTION 131

- (Topic 2)

A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

- A. Use S3 Object Lock In governance mode with a legal hold of 1 year
- B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
- C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket Use an S3 bucket policy to only allow the IAM role
- D. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added Configure the function to track the hash of the saved object to that modified objects can be marked accordingly

Answer: B

Explanation:

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period. In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. In Governance mode, Objects can be deleted by some users with special permissions, this is against the requirement.

Compliance:

- Object versions can't be overwritten or deleted by any user, including the root user

- Objects retention modes can't be changed, and retention periods can't be shortened

Governance:

- Most users can't overwrite or delete an object version or alter its lock settings
- Some users have special permissions to change the retention or delete the object

NEW QUESTION 135

- (Topic 2)

A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.

Which solutions will meet these requirements? (Choose two.)

- A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
- B. Use rules in AWS WAF to prevent internet access
- C. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
- D. Use AWS Organizations to configure service control policies (SCPs) that prevent VPCs from gaining internet access
- E. Deny access to all AWS Regions except ap-northeast-3.
- F. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
- G. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Answer: AC

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_vpc.html#example_vpc_2

NEW QUESTION 136

- (Topic 2)

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

- A. Use Spot Instances for the data ingestion layer
- B. Use On-Demand Instances for the data ingestion layer
- C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
- D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
- E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Answer: AC

Explanation:

EC2 instance Savings Plan saves 72% while Compute Savings Plans saves 66%. But according to link, it says "Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage." EC2 instance Savings Plans are not applied to Fargate or Lambda

NEW QUESTION 138

- (Topic 2)

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.

Which solution meets these requirements MOST cost-effectively?

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

Answer: C

Explanation:

This solution meets the requirements of a disaster recovery solution to back up the data that is generated by an analytics application, stored in JSON format, and must be accessible in milliseconds if it is needed. Amazon S3 Standard is a durable and scalable storage class for frequently accessed data. It can store any amount of data and provide high availability and performance. It can also support millisecond access time for data retrieval.

Option A is incorrect because Amazon OpenSearch Service (Amazon Elasticsearch Service) is a search and analytics service that can index and query data, but it is not a backup solution for data stored in JSON format. Option B is incorrect because Amazon S3 Glacier is a low-cost storage class for data archiving and long-term backup, but it does not support millisecond access time for data retrieval. Option D is incorrect because Amazon RDS for PostgreSQL is a relational database service that can store and query structured data, but it is not a backup solution for data stored in JSON format.

References:

? <https://aws.amazon.com/s3/storage-classes/>

? https://aws.amazon.com/s3/faqs/#Durability_and_data_protection

NEW QUESTION 141

- (Topic 2)

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants a new solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality
- B. Create and deploy an AWS Lambda function to manage and serve the website content
- C. Create the new website and an Amazon S3 bucket Deploy the website on the S3 bucket with static website hosting enabled
- D. Create the new website
- E. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Answer: AD

Explanation:

A -> We can configure CloudFront to require HTTPS from clients (enhanced security)
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html> D -> storing static website on S3 provides scalability and less operational overhead, then configuration of Application LB and EC2 instances (hence E is out)

NEW QUESTION 145

- (Topic 2)

A company wants to build a scalable key management Infrastructure to support developers who need to encrypt data in their applications. What should a solutions architect do to reduce the operational burden?

- A. Use multifactor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys

Answer: B

Explanation:

<https://aws.amazon.com/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs%20to%20digitally,a%20broad%20set%20of%20industry%20and%20regional%20compliance%20regimes.>

NEW QUESTION 149

- (Topic 2)

A company wants to measure the effectiveness of its recent marketing campaigns. The company performs batch processing on csv files of sales data and stores the results in an Amazon S3 bucket once every hour. The S3 bucket contains petabytes of objects. The company runs one-time queries in Amazon Athena to determine which products are most popular on a particular date for a particular region. Queries sometimes fail or take longer than expected to finish. Which actions should a solutions architect take to improve the query performance and reliability? (Select TWO.)

- A. Reduce the S3 object sizes to less than 126 MB
- B. Partition the data by date and region in Amazon S3
- C. Store the files as large, single objects in Amazon S3.
- D. Use Amazon Kinesis Data Analytics to run the Queries as part of the batch processing operation
- E. Use an AWS Glue extract, transform, and load (ETL) process to convert the csv files into Apache Parquet format.

Answer: BE

Explanation:

<https://aws.amazon.com/blogs/big-data/top-10-performance-tuning-tips-for-amazon-athena/>
This solution meets the requirements of measuring the effectiveness of marketing campaigns by performing batch processing on csv files of sales data and storing the results in an Amazon S3 bucket once every hour. An AWS Glue ETL process can use services such as AWS Glue or AWS Data Pipeline to extract data from S3, transform it into a more efficient format such as Apache Parquet, and load it back into S3. Apache Parquet is a columnar storage format that can improve the query performance and reliability of Athena by reducing the amount of data scanned, improving compression ratio, and enabling predicate pushdown.

NEW QUESTION 150

- (Topic 2)

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege. Which steps should the solutions architect do in conjunction to reach this goal? (Select two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrators/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using the IAM role.

Answer: DE

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

NEW QUESTION 155

- (Topic 2)

A company is planning to build a high performance computing (HPC) workload as a service solution that is hosted on AWS. A group of 16 Amazon EC2 Linux Instances requires the lowest possible latency for node-to-node communication. The instances also need a shared block device volume for high-performing storage. Which solution will meet these requirements?

- A. Use a distributed placement group
- B. Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach
- C. Use a cluster placement group

- D. Create shared file systems across the instances by using Amazon Elastic File System (Amazon EFS)
- E. Use a partition placement group
- F. Create shared file systems across the instances by using Amazon Elastic File System (Amazon EFS).
- G. Use a spread placement group
- H. Attach a single Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume to all the instances by using Amazon EBS Multi-Attach

Answer: A

Explanation:

- 1. lowest possible latency + node to node ==> cluster placement(must be within one AZ), so C, D out
- * 2. For EBS Multi-Attach, up to 16 instances can be attached to a single volume==>we have 16 linux instance==>more close to A
- * 3. "need a shared block device volume"==>EBS Multi-attach is Block Storage whereas EFS is File Storage==> B out
- * 4. EFS automatically replicates data within and across 3 AZ==>we use cluster placement so all EC2 are within one AZ.
- * 5. EBS Multi-attach volumes can be used for clients within a single AZ. <https://repost.aws/questions/QUK2RANw1QTKCwpDUwCCi72A/efs-vs-ebs-mult-attach>

NEW QUESTION 159

- (Topic 2)

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

- A. Create a new S3 bucket
- B. Load the data into the new S3 bucket
- C. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region
- D. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon Athena to query the data.
- E. Create a new S3 bucket
- F. Load the data into the new S3 bucket
- G. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region
- H. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.
- I. Load the data into the existing S3 bucket
- J. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region
- K. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
- L. Load the data into the existing S3 bucket
- M. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region
- N. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

Answer: A

Explanation:

This solution meets the requirements of a serverless solution, encryption, replication, and SQL analysis with the least operational overhead. Amazon Athena is a serverless interactive query service that can analyze data in S3 using standard SQL. S3 Cross-Region Replication (CRR) can replicate encrypted objects to an S3 bucket in another Region automatically. Server-side encryption with AWS KMS multi-Region keys (SSE-KMS) can encrypt the data at rest using keys that are replicated across multiple Regions. Creating a new S3 bucket can avoid potential conflicts with existing data or configurations.

Option B is incorrect because Amazon RDS is not a serverless solution and it cannot query data in S3 directly. Option C is incorrect because server-side encryption with Amazon S3 managed encryption keys (SSE-S3) does not use KMS keys and it does not support multi-Region replication. Option D is incorrect because Amazon RDS is not a serverless solution and it cannot query data in S3 directly. It is also incorrect for the same reason as option C. References:

? <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-walkthrough-4.html>

? <https://aws.amazon.com/blogs/storage/considering-four-different-replication-options-for-data-in-amazon-s3/>

? <https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>

? <https://aws.amazon.com/athena/>

NEW QUESTION 161

- (Topic 2)

A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

- A. Configure the Lambda function to run in the VPC with the appropriate security group.
- B. Set up a VPN connection from AWS to the data center
- C. Route the traffic from the Lambda function through the VPN.
- D. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
- E. Create an Elastic IP address
- F. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Answer: A

Explanation:

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>

NEW QUESTION 164

- (Topic 2)

A company has an event-driven application that invokes AWS Lambda functions up to 800 times each minute with varying runtimes. The Lambda functions access data that is stored in an Amazon Aurora MySQL DB cluster. The company is noticing connection timeouts as user activity increases. The database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low.

Which solution will resolve this issue with the LEAST operational overhead?

- A. Adjust the size of the Aurora MySQL nodes to handle more connections

- B. Configure retry logic in the Lambda functions for attempts to connect to the database
- C. Set up Amazon ElastiCache for Redis to cache commonly read items from the database
- D. Configure the Lambda functions to connect to ElastiCache for reads.
- E. Add an Aurora Replica as a reader node
- F. Configure the Lambda functions to connect to the reader endpoint of the DB cluster rather than to the writer endpoint.
- G. Use Amazon ROS Proxy to create a proxy
- H. Set the DB cluster as the target database. Configure the Lambda functions to connect to the proxy rather than to the DB cluster.

Answer: D

Explanation:

1. database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low==>A and C out. We cannot only add nodes instance or add read replica, because database workload is totally fine, very low. 2. "least operational overhead"==>B out, because b need to configure lambda. 3. ROS proxy: Shares infrequently used connections; High availability with failover; Drives increased efficiency==>proxy can leverage failover to redirect traffic from timeout rds instance to healthy rds instance. So D is right.

NEW QUESTION 168

- (Topic 2)

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide are accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Answer: B

Explanation:

ElastiCache, enhances the performance of web applications by quickly retrieving information from fully-managed in-memory data stores. It utilizes Memcached and Redis, and manages to considerably reduce the time your applications would, otherwise, take to read data from disk-based databases. Amazon CloudFront supports dynamic content from HTTP and WebSocket protocols, which are based on the Transmission Control Protocol (TCP) protocol. Common use cases include dynamic API calls, web pages and web applications, as well as an application's static files such as audio and images. It also supports on-demand media streaming over HTTP. AWS Global Accelerator supports both User Datagram Protocol (UDP) and TCP-based protocols. It is commonly used for non- HTTP use cases, such as gaming, IoT and voice over IP. It is also good for HTTP use cases that need static IP addresses or fast regional failover

NEW QUESTION 172

- (Topic 2)

An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts and the application did not process the orders of those customers. A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

- A. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.
- B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.
- C. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.
- D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

Answer: B

Explanation:

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. <https://aws.amazon.com/id/rds/proxy/>

NEW QUESTION 175

- (Topic 2)

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

How should the solutions architect comply with these requirements?

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-aws-waf.html>

NEW QUESTION 176

- (Topic 2)

A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases. What should a solutions architect do to meet these requirements?

- A. Attach a Network Load Balancer to the Auto Scaling group
- B. Attach an Application Load Balancer to the Auto Scaling group.
- C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately
- D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Answer: A

Explanation:

This solution meets the requirements of running a gaming application that transmits data by using UDP packets and scaling out and in as traffic increases and decreases. A Network Load Balancer can handle millions of requests per second while maintaining high throughput at ultra low latency, and it supports both TCP and UDP protocols. An Auto Scaling group can automatically adjust the number of EC2 instances based on the demand and the scaling policies. Option B is incorrect because an Application Load Balancer does not support UDP protocol, only HTTP and HTTPS. Option C is incorrect because Amazon Route 53 is a DNS service that can route traffic based on different policies, but it does not provide load balancing or scaling capabilities. Option D is incorrect because a NAT instance is used to enable instances in a private subnet to connect to the internet or other AWS services, but it does not provide load balancing or scaling capabilities.

References:

? <https://aws.amazon.com/blogs/aws/new-udp-load-balancing-for-network-load-balancer/>

? <https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

NEW QUESTION 181

- (Topic 2)

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

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

Answer: C

Explanation:

<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

NEW QUESTION 182

- (Topic 2)

A company has a data ingestion workflow that includes the following components:

- An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries
- An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues. When a failure occurs the corresponding data is not ingested unless the company manually reruns the job. What should a solutions architect do to ensure that all notifications are eventually processed?

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

NEW QUESTION 184

- (Topic 2)

A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly. Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the database to an Amazon RDS for MySQL DB instance
- B. Create an AMI of the web application
- C. Use the AMI to launch a second EC2 On-Demand Instance
- D. Use an Application Load Balancer to distribute the load to each EC2 instance.
- E. Migrate the database to an Amazon RDS for MySQL DB instance
- F. Create an AMI of the web application
- G. Use the AMI to launch a second EC2 On-Demand Instance
- H. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
- I. Migrate the database to an Amazon Aurora MySQL DB instance
- J. Create an AWS Lambda function to stop the EC2 instance and change the instance type
- K. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
- L. Migrate the database to an Amazon Aurora MySQL DB instance
- M. Create an AMI of the web application

- N. Apply the AMI to a launch template
- O. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet
- P. Attach an Application Load Balancer to the Auto Scaling group.

Answer: D

Explanation:

Migrate the database to Amazon Aurora MySQL - this will let the DB scale on it's own; it'll scale automatically without needing adjustment. Create AMI of the web app and using a launch template - this will make the creating of any future instances of the app seamless. They can then be added to the auto scaling group which will save them money as it will scale up and down based on demand. Using a spot fleet to launch instances- This solves the "MOST cost-effective" portion of the question as spot instances come at a huge discount at the cost of being terminated at any time Amazon deems fit. I think this is why there's a bit of disagreement on this. While it's the most cost effective, it would be a terrible choice if amazon were to terminate that spot instance during a busy period.

NEW QUESTION 187

- (Topic 2)

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL. What should a solutions architect do to meet these requirements?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user
- C. Grant the user read permission to objects in the S3 bucket
- D. Assign the user to CloudFront.
- E. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- F. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution
- G. Configure the S3 bucket permissions so that only the OAI has read permission.

Answer: D

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html#private-content-restricting-access-to-s3-overview>

NEW QUESTION 192

- (Topic 2)

A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks. Which solution will meet these requirements with the LEAST amount of administrative effort?

- A. Set up AWS WAF in both Region
- B. Associate Regional web ACLs with an API stage.
- C. Set up AWS Firewall Manager in both Region
- D. Centrally configure AWS WAF rules.
- E. Set up AWS Shield in both Region
- F. Associate Regional web ACLs with an API stage.
- G. Set up AWS Shield in one of the Region
- H. Associate Regional web ACLs with an API stage.

Answer: A

Explanation:

Using AWS WAF has several benefits. Additional protection against web attacks using criteria that you specify. You can define criteria using characteristics of web requests such as the following: Presence of SQL code that is likely to be malicious (known as SQL injection). Presence of a script that is likely to be malicious (known as cross-site scripting). AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections. <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

NEW QUESTION 197

- (Topic 2)

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application's performance?

- A. Create a new SSL certificate using AWS Certificate Manager (ACM) install the ACM certificate on each instance
- B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket Configure the EC2 instances to reference the bucket for SSL termination
- C. Create another EC2 instance as a proxy server Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances
- D. Import the SSL certificate into AWS Certificate Manager (ACM) Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM

Answer: D

Explanation:

<https://aws.amazon.com/certificate-manager/>:

"With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACM- integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally."

NEW QUESTION 201

- (Topic 2)

A company runs its ecommerce application on AWS. Every new order is published as a message in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone.

The company needs to redesign its architecture to provide the highest availability with the least operational overhead.

What should a solutions architect do to meet these requirements?

- A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon M
- B. Create a Multi-AZ Auto Scaling group (or EC2 instances that host the applicatio
- C. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
- D. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon M
- E. Create a Multi-AZ Auto Scaling group for EC2 instances that host the applicatio
- F. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- G. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queu
- H. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- I. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the applicatio
- J. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.

Answer: B

Explanation:

Migrating to Amazon MQ reduces the overhead on the queue management. C and D are dismissed. Deciding between A and B means deciding to go for an AutoScaling group for EC2 or an RDS for Postgress (both multi- AZ). The RDS option has less operational impact, as provide as a service the tools and software required. Consider for instance, the effort to add an additional node like a read replica, to the DB. <https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html> <https://aws.amazon.com/rds/postgresql/>

NEW QUESTION 203

- (Topic 2)

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

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

- A. Replace the EC2 instances with T3 EC2 instances that run in an Auto Scaling group
- B. Make the changes by using the AWS Management Console.
- C. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group
- D. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary
- E. Modify the CloudFormation template
- F. Replace the EC2 instances with R5 EC2 instance
- G. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
- H. Modify the CloudFormation template
- I. Replace the EC2 instances with R5 EC2 instance
- J. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

Answer: D

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/>

NEW QUESTION 207

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SAA-C03 Practice Exam Features:

- * SAA-C03 Questions and Answers Updated Frequently
- * SAA-C03 Practice Questions Verified by Expert Senior Certified Staff
- * SAA-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SAA-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SAA-C03 Practice Test Here](#)